Privacy Impact Assessment
for the

Critical Infrastructure Change Detection

June 19, 2008

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

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

Abstract

The Critical Infrastructure Change Detection (CICD) 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 the system demonstration will be performed in a public area of New York City 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."

The Critical Infrastructure Change Detection program 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 that total situational awareness of the surrounding area is critical. A threat may involve people casing a facility, carrying unusual items, etc. For this project, algorithms are not being tested at this time to discriminate attributes of individuals (clothing, facial features, behavior). Here, the focus is on developing a system with the hardware and optical resolution that may ultimately better facilitate such detection.

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 being developed 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 allowing 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 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.

S&T anticipates collecting and retaining 24-48 hours of images for this project. The rest of the week-long period will be dedicated setup, system calibration, and removal. Retaining 24-48 hours of images is important to the project because rapid-scan forensic analysis (e.g., how may vehicles entered Area 1 in a 24 hour period) is an important feature of the system.

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 a partnership with the New York Police Department (NYPD) for the CICD project.

The demonstration is not a law enforcement exercise. NYPD will be present to evaluate the utility of the technology and provide feedback to DHS, but will not be making operational law enforcement decisions. NYPD will provide user requirements for the system and will evaluate system effectiveness during the project demonstration.

The demonstration will occur in Foley Square in New York City, an area recommended by the NYPD in which NYPD cameras are already operating.. The system will be temporarily installed and operated in Foley Square for approximately 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 manually cued images, change detection in exclusion zones, and semi-automated forensic analysis). The CICD system will be installed in a trailer and will be operated by personnel from the Labs, S&T, and NYPD. The trailer containing computers, operator stations, and the optical sensor will be configured at MIT Lincoln Laboratory, brought to Foley Square and positioned near the perimeter of the Square in such a way to optimally collect images without significantly impeding pedestrian traffic. Signs will be posted in several locations throughout the Square. The optical sensor (i.e., the camera) will be mounted on a mast attached to the trailer that can be extended to a maximum height of 50 feet. Monitors installed in the trailer will allow multiple users to simultaneously operate the system.

Lab personnel will be the primary operators, as they best understand system operation. S&T and NYPD will operate the system for the purpose of evaluating its effectiveness and providing feedback to the labs to help guide future system development. The NYPD will not make any operational, law enforcement decisions and will not engage in any law enforcement actions based on the CICD test system.

Following the demonstration, Lab personnel will remove the trailer containing the CICD system from Foley Square and collect technical evaluation data from the NYPD and the S&T program manager. The effectiveness of the system in this first demonstration will guide further development and addition of capabilities. The CICD system and the images collected during the test will only be used for research and development purposes.

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: 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 the identity of the individual or any other identifying characteristics of particular individuals, just the technical ability to track one person in a crowd of people.
- ☐ 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).
- ☐ 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 vehicles into and out of a access-controlled street. Change detection algorithms are being developed that will attempt to detect a vehicle that has entered the targeted street. Images of people also will be captured as part of the demonstration and system evaluation, but specific populations will not be targeted by specific attributes (such as by clothing, physical appearance, etc).

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 key 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). 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 is 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.

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 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 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 Department of Homeland Security, MIT Lincoln Laboratory (LL), and/or Pacific Northwest National Laboratory (PNNL) and have a

legitimate need to access the images. The Project Manager will grant access to the images only after demonstrating a legitimate need. MIT Lincoln Laboratory and Pacific Northwest National Laboratory will store the images. While not in use, the labs 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 have IT security measures in place to ensure that the laboratory 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, LL, and PNNL employees as described above). For example, the NYPD will only view the video images at the time the images are recorded and during subsequent project evaluation meeting 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, LL, and PNNL) with physical security provided by the New York Police Department.

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 and FY08 DHS S&T Appropriations
☐ Funding renewal is contingent on program evaluation

Appendix is attached, including:
- ☒ Authorizing legislation – Title 3 of the Homeland Security Act
- ☐ 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 and the labs will use the video collected during the CICD demonstration for research and development purposes only. This demonstration is intended to demonstrate the capability of the surveillance technology to local law enforcement. S&T and the labs will not target specific individuals based on pre-determined attributes, nor will S&T and the labs 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 building interiors or other 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 would 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 NYPD 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. NYPD will not engage in any 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, NYPD, 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 and the labs will use the images to evaluate system performance (digital image stitching for complex scenes, resolution, effectiveness of tracking manually 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.

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 and the labs prior to the demonstration. S&T will also brief individual observers from the New York Police Department 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.

Image archives will be physically stored at MIT Lincoln Laboratory and Pacific Northwest National Laboratory. Access to the images will be granted by the appropriate Project Manager only after demonstrating 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. Lincoln Laboratory and Pacific Northwest National Laboratory, 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 first demonstration phase and to make improvements in future phases of the project. The labs 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.

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 first demonstration phase and to make improvements in future phases of the project. The labs 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 and the Labs 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 MIT Lincoln Laboratory and Pacific Northwest National Laboratory. 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 CICD privacy guidance (attached), 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) – New York Police Department
☐ 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)
- ☐ 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

New York Police Department (NYPD) – S&T will share the live-feed images with NYPD 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 NYPD defining their highest priority needs. NYPD personnel will participate in the demonstration and will thereby have access to images feeds at the demonstration site. In addition, NYPD 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, Lincoln Laboratory – The images collected from the demonstration will only be used by authorized project personnel at Pacific Northwest National Laboratory and Lincoln Laboratory for research and development activities in accordance with the approved Statements of Work in the contracts with DHS. 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.

S&T is sharing the information pursuant to Subchapter 3 §182 of the Homeland Security Act, which assigns the Under Secretary for Science and Technology the responsibility for conducting basic and applied research, development, demonstration, testing, and evaluation activities.

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

- ☒ Discrete portions of video 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 NYPD. However, participating NYPD personnel will be required to participate in a training briefing along with a copy of this PIA as required reading.

Pacific Northwest National Laboratory and MIT Lincoln Laboratory 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 with a demonstrated "need to know." S&T will require all participants in the research, including lab personnel and NYPD, to read and sign the CICD Privacy Guidelines (attached). The labs will 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 demonstration (physically present in the trailer housing the CICD system) will have access to the real-time images. This includes personnel from the Labs, S&T, and NYPD.
☐ 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 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 NYPD 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 read this PIA 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 Lincoln Laboratory and Pacific Northwest National Laboratory. Access to the images will be granted by the appropriate Project Manager at the respective laboratory only after demonstrating 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 period of approximately one week. 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. Lincoln Laboratory and Pacific Northwest National Laboratory, 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, Lincoln Laboratory and Pacific Northwest National Laboratory have IT security measures in place to ensure that images is 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 will restrict access to the images to authorized individuals with a demonstrated need to know. The labs 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
☒ Attached 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 Privacy Impact Assessment and evaluate the appropriateness of such design choices.

Responsible Officials

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

Approval Signature

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

APPENDIX A: Authorizing Legislation

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

SEC. 301. UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.
There shall be in the Department a Directorate of Science and Technology headed by an Under Secretary for Science and Technology.

SEC. 302. RESPONSIBILITIES AND AUTHORITIES OF THE UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.
The Secretary, acting through the Under Secretary for Science and Technology, shall have the responsibility for—
(1) advising the Secretary regarding research and development efforts and priorities in support of the Department's missions;
(2) developing, in consultation with other appropriate executive agencies, a national policy and strategic plan for, identifying priorities, goals, objectives and policies for, and coordinating the Federal Government's civilian efforts to identify and develop countermeasures to chemical, biological, radiological, nuclear, and other emerging terrorist threats, including the development of comprehensive, research-based definable goals for such efforts and development of annual measurable objectives and specific targets to accomplish and evaluate the goals for such efforts;
(3) supporting the Under Secretary for Information Analysis and Infrastructure Protection, by assessing and testing homeland security vulnerabilities and possible threats;
(4) conducting 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, except that such responsibility does not extend to human health-related research and development activities;
(5) establishing priorities for, directing, funding, and conducting national research, development, test and evaluation, and procurement of technology and systems for—
(A) preventing the importation of chemical, biological, radiological, nuclear, and related weapons and material; and
(B) detecting, preventing, protecting against, and responding to terrorist attacks;
(6) establishing a system for transferring homeland security developments or technologies to Federal, State, local government, and private sector entities;
(7) entering into work agreements, joint sponsorships, contracts, or any other agreements with the Department of Energy regarding the use of the national laboratories or sites and
support of the science and technology base at those facilities;
(8) collaborating with the Secretary of Agriculture and the Attorney General as provided in section 212 of the Agricultural Bioterrorism Protection Act of 2002 (7 U.S.C. 8401), as amended by section 1709(b);
(9) collaborating with the Secretary of Health and Human Services and the Attorney General in determining any new biological agents and toxins that shall be listed as ''select agents'' in Appendix A of part 72 of title 42, Code of Federal Regulations, pursuant to section 351A of the Public Health Service Act (42 U.S.C. 262a);
(10) supporting United States leadership in science and technology;
(11) establishing and administering the primary research and development activities of the Department, including the long-term research and development needs and capabilities for all elements of the Department;
(12) coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department;
(13) coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs; and

(14) developing and overseeing the administration of guidelines for merit review of research and development projects throughout the Department, and for the dissemination of research conducted or sponsored by the Department.

SEC. 303. FUNCTIONS TRANSFERRED.
In accordance with title XV, there shall be transferred to the Secretary the functions, personnel, assets, and liabilities of the following entities:
(1) The following programs and activities of the Department of Energy, including the functions of the Secretary of Energy relating thereto (but not including programs and activities relating to the strategic nuclear defense posture of the United States):
(A) The chemical and biological national security and supporting programs and activities of the nonproliferation and verification research and development program.
(B) The nuclear smuggling programs and activities within the proliferation detection program of the nonproliferation and verification research and development program. The programs and activities described in this subparagraph may be designated by the President either for transfer to the Department or for joint operation by the Secretary and the Secretary of Energy.
(C) The nuclear assessment program and activities of the assessment, detection, and cooperation program of the international materials protection and cooperation program.
(D) Such life sciences activities of the biological and environmental research program related to microbial pathogens as may be designated by the President for transfer to the Department.
(E) The Environmental Measurements Laboratory.
(F) The advanced scientific computing research program and activities at Lawrence Livermore National Laboratory.
(2) The National Bio-Weapons Defense Analysis Center of the Department of Defense, including the functions of the Secretary of Defense related thereto.

SEC. 304. CONDUCT OF CERTAIN PUBLIC HEALTH-RELATED ACTIVITIES.
(a) IN GENERAL.—With respect to civilian human health-related research and development activities relating to countermeasures for chemical, biological, radiological, and nuclear and other emerging terrorist threats carried out by the Department of Health and Human Services (including the Public Health Service), the Secretary of Health and Human Services shall set priorities, goals, objectives, and policies and develop a coordinated strategy for such activities in collaboration with the Secretary of Homeland Security to ensure consistency with the national policy and strategic plan developed pursuant to section 302(2).
(b) EVALUATION OF PROGRESS.—In carrying out subsection (a), the Secretary of Health and Human Services shall collaborate with the Secretary in developing specific benchmarks and outcome measurements for evaluating progress toward achieving the priorities and goals described in such subsection.
(c) ADMINISTRATION OF COUNTERMEASURES AGAINST SMALLPOX.—Section 224 of the Public Health Service Act (42 U.S.C. 233) is amended by adding the following:
''(p) ADMINISTRATION OF SMALLPOX COUNTERMEASURES BY HEALTH PROFESSIONALS.—
''(1) IN GENERAL.—For purposes of this section, and subject to other provisions of this subsection, a covered person shall be deemed to be an employee of the Public Health Service with respect to liability arising out of administration of a covered countermeasure against smallpox to an individual during the effective period of a declaration by the Secretary under paragraph (2)(A).
''(2) DECLARATION BY SECRETARY CONCERNING COUNTERMEASURE AGAINST SMALLPOX.—
''(A) AUTHORITY TO ISSUE DECLARATION.—
''(i) IN GENERAL.—The Secretary may issue a declaration, pursuant to this paragraph, concluding that an actual or potential bioterrorist incident or other actual or potential public health emergency makes advisable the administration of a covered countermeasure to a category or categories of individuals.

''(ii) COVERED COUNTERMEASURE.—The Secretary shall specify in such declaration the substance or substances that shall be considered covered countermeasures (as defined in paragraph (8)(A)) for purposes of administration to individuals during the effective period of the declaration.
''(iii) EFFECTIVE PERIOD.—The Secretary shall specify in such declaration the beginning and ending dates of the effective period of the declaration, and may subsequently amend such declaration to shorten or extend such effective period, provided that the new closing date is after the date when the declaration is amended.
''(iv) PUBLICATION.—The Secretary shall promptly publish each such declaration and amendment in the Federal Register.
''(B) LIABILITY OF UNITED STATES ONLY FOR ADMINISTRATIONS WITHIN SCOPE OF DECLARATION.—Except as provided in paragraph (5)(B)(ii), the United States shall be liable under this subsection with respect to a claim arising out of the administration of a covered countermeasure to an individual only if—
''(i) the countermeasure was administered by a qualified person, for a purpose stated in paragraph (7)(A)(i), and during the effective period of a declaration by the Secretary under subparagraph (A) with respect to such countermeasure; and
''(ii)(I) the individual was within a category of individuals covered by the declaration; or
''(II) the qualified person administering the countermeasure had reasonable grounds to believe that such individual was within such category.
''(C) PRESUMPTION OF ADMINISTRATION WITHIN SCOPE OF DECLARATION IN CASE OF ACCIDENTAL VACCINIA INOCULATION.—
''(i) IN GENERAL.—If vaccinia vaccine is a covered countermeasure specified in a declaration under subparagraph (A), and an individual to whom the vaccinia vaccine is not administered contracts vaccinia, then, under the circumstances specified in clause (ii), the individual—
''(I) shall be rebuttably presumed to have contracted vaccinia from an individual to whom such vaccine was administered as provided by clauses (i) and (ii) of subparagraph (B); and ''(II) shall (unless such presumption is rebutted) be deemed for purposes of this subsection to be an individual to whom a covered countermeasure was administered by a qualified person in accordance with the terms of such declaration and as described by subparagraph (B).
''(ii) CIRCUMSTANCES IN WHICH PRESUMPTION
APPLIES.—The presumption and deeming stated in clause (i) shall apply if—
''(I) the individual contracts vaccinia during the effective period of a declaration under subparagraph (A) or by the date 30 days after the close of such period; or
''(II) the individual resides or has resided with an individual to whom such vaccine was administered as provided by clauses (i) and (ii) of subparagraph (B) and contracts vaccinia after such date.
''(3) EXCLUSIVITY OF REMEDY.—The remedy provided by subsection (a) shall be exclusive of any other civil action or proceeding for any claim or suit this subsection encompasses.
''(4) CERTIFICATION OF ACTION BY ATTORNEY GENERAL.—
Subsection (c) applies to actions under this subsection, subject to the following provisions:
Federal Register, publication.
''(A) NATURE OF CERTIFICATION.—The certification by the Attorney General that is the basis for deeming an action or proceeding to be against the United States, and for removing an action or proceeding from a State court, is a certification that the action or proceeding is against a covered person and is based upon a claim alleging personal injury or death arising out of the administration of a covered countermeasure.
''(B) CERTIFICATION OF ATTORNEY GENERAL CONCLUSIVE.—
The certification of the Attorney General of the facts specified in subparagraph (A) shall conclusively establish such facts for purposes of jurisdiction pursuant to this subsection.
''(5) DEFENDANT TO COOPERATE WITH UNITED STATES.—

''(A) IN GENERAL.—A covered person shall cooperate with the United States in the processing and defense of a claim or action under this subsection based upon alleged acts or omissions of such person.
''(B) CONSEQUENCES OF FAILURE TO COOPERATE.—Upon the motion of the United States or any other party and upon finding that such person has failed to so cooperate—
''(i) the court shall substitute such person as the party defendant in place of the United States and, upon motion, shall remand any such suit to the court in which it was instituted if it appears that the court lacks subject matter jurisdiction;
''(ii) the United States shall not be liable based on the acts or omissions of such person; and
''(iii) the Attorney General shall not be obligated to defend such action.
''(6) RECOURSE AGAINST COVERED PERSON IN CASE OF GROSS MISCONDUCT OR CONTRACT VIOLATION.—
''(A) IN GENERAL.—Should payment be made by the United States to any claimant bringing a claim under this subsection, either by way of administrative determination, settlement, or court judgment, the United States shall have, notwithstanding any provision of State law, the right to recover for that portion of the damages so awarded or paid, as well as interest and any costs of litigation, resulting from the failure of any covered person to carry out any obligation or responsibility assumed by such person under a contract with the United States or from any grossly negligent, reckless, or illegal conduct or willful misconduct on the part of such person.
''(B) VENUE.—The United States may maintain an action under this paragraph against such person in the district court of the United States in which such person resides or has its principal place of business.
''(7) DEFINITIONS.—As used in this subsection, terms have the following meanings:
''(A) COVERED COUNTERMEASURE.—The term 'covered countermeasure' or 'covered countermeasure against smallpox', means a substance that is—
''(i)(I) used to prevent or treat smallpox (including the vaccinia or another vaccine); or
''(II) vaccinia immune globulin used to control or treat the adverse effects of vaccinia inoculation; and
''(ii) specified in a declaration under paragraph (2).
''(B) COVERED PERSON.—The term 'covered person', when used with respect to the administration of a covered countermeasure, includes any person who is—
''(i) a manufacturer or distributor of such countermeasure;
''(ii) a health care entity under whose auspices such countermeasure was administered;
''(iii) a qualified person who administered such countermeasure; or
''(iv) an official, agent, or employee of a person described in clause (i), (ii), or (iii).
''(C) QUALIFIED PERSON.—The term 'qualified person', when used with respect to the administration of a covered countermeasure, means a licensed health professional or other individual who is authorized to administer such countermeasure under the law of the State in which the countermeasure was administered.''.

SEC. 305. FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS.
The Secretary, acting through the Under Secretary for Science and Technology, shall have the authority to establish or contract with 1 or more federally funded research and development centers to provide independent analysis of homeland security issues, or to carry out other responsibilities under this Act, including coordinating and integrating both the extramural and intramural programs described in section 308.

SEC. 306. MISCELLANEOUS PROVISIONS.
(a) CLASSIFICATION.—To the greatest extent practicable, research conducted or supported by the Department shall be unclassified.
(b) CONSTRUCTION.—Nothing in this title shall be construed to preclude any Under Secretary of the Department from carrying out research, development, demonstration, or deployment activities, as long as such activities are coordinated through the Under Secretary for Science and Technology.

(c) REGULATIONS.—The Secretary, acting through the Under Secretary for Science and Technology, may issue necessary regulations with respect to research, development, demonstration, testing, and evaluation activities of the Department, including the conducting, funding, and reviewing of such activities.
(d) NOTIFICATION OF PRESIDENTIAL LIFE SCIENCES DESIGNATIONS.—
Not later than 60 days before effecting any transfer of Department of Energy life sciences activities pursuant to section 303(1)(D) of this Act, the President shall notify the appropriate congressional committees of the proposed transfer and shall include the reasons for the transfer and a description of the effect of the transfer on the activities of the Department of Energy.

SEC. 307. HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY.
(a) DEFINITIONS.—In this section:
(1) FUND.—The term ''Fund'' means the Acceleration Fund for Research and Development of Homeland Security Technologies established in subsection (c).
(2) HOMELAND SECURITY RESEARCH.—The term ''homeland security research'' means research relevant to the detection of, prevention of, protection against, response to, attribution of, and recovery from homeland security threats, particularly acts of terrorism.
(3) HSARPA.—The term ''HSARPA'' means the Homeland Security Advanced Research Projects Agency established in subsection (b).
(4) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary for Science and Technology.
(b) HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY.—
(1) ESTABLISHMENT.—There is established the Homeland Security Advanced Research Projects Agency.
(2) DIRECTOR.—HSARPA shall be headed by a Director, who shall be appointed by the Secretary. The Director shall report to the Under Secretary.
(3) RESPONSIBILITIES.—The Director shall administer the Fund to award competitive, merit-reviewed grants, cooperative agreements or contracts to public or private entities, including businesses, federally funded research and development centers, and universities. The Director shall administer the Fund to—
(A) support basic and applied homeland security research to promote revolutionary changes in technologies that would promote homeland security;
(B) advance the development, testing and evaluation, and deployment of critical homeland security technologies; and
(C) accelerate the prototyping and deployment of technologies that would address homeland security vulnerabilities.
(4) TARGETED COMPETITIONS.—The Director may solicit proposals to address specific vulnerabilities identified by the Director.
(5) COORDINATION.—The Director shall ensure that the activities of HSARPA are coordinated with those of other relevant research agencies, and may run projects jointly with other agencies.
(6) PERSONNEL.—In hiring personnel for HSARPA, the Secretary shall have the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261). The term of appointments for employees under subsection (c)(1) of that section may not exceed 5 years before the granting of any extension under subsection (c)(2) of that section.
(7) DEMONSTRATIONS.—The Director, periodically, shall hold homeland security technology demonstrations to improve contact among technology developers, vendors and acquisition personnel.
(c) FUND.—
(1) ESTABLISHMENT.—There is established the Acceleration Fund for Research and Development of Homeland Security Technologies, which shall be administered by the Director of HSARPA.
(2) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $500,000,000 to the Fund for fiscal year 2003 and such sums as may be necessary thereafter.

(3) COAST GUARD.—Of the funds authorized to be appropriated under paragraph (2), not less than 10 percent of such funds for each fiscal year through fiscal year 2005 shall be authorized only for the Under Secretary, through joint agreement with the Commandant of the Coast Guard, to carry out research and development of improved ports, waterways and coastal security surveillance and perimeter protection capabilities for the purpose of minimizing the possibility that Coast Guard cutters, aircraft, helicopters, and personnel will be diverted from non-homeland security missions to the ports, waterways and coastal security mission.

SEC. 308. CONDUCT OF RESEARCH, DEVELOPMENT, DEMONSTRATION, TESTING AND EVALUATION.
(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall carry out the responsibilities under section 302(4) through both extramural and intramural programs.
(b) EXTRAMURAL PROGRAMS.—
(1) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall operate extramural research, development, demonstration, testing, and evaluation programs so as to—
(A) ensure that colleges, universities, private research institutes, and companies (and consortia thereof) from as many areas of the United States as practicable participate;
(B) ensure that the research funded is of high quality, as determined through merit review processes developed under section 302(14); and
(C) distribute funds through grants, cooperative agreements, and contracts.
(2) UNIVERSITY-BASED CENTERS FOR HOMELAND SECURITY.—
(A) ESTABLISHMENT.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish within 1 year of the date of enactment of this Act a university-based center or centers for homeland security. The purpose of this center or centers shall be to establish a coordinated, university-based system to enhance the Nation's homeland security.
(B) CRITERIA FOR SELECTION.—In selecting colleges or universities as centers for homeland security, the Secretary shall consider the following criteria:
(i) Demonstrated expertise in the training of first responders.
(ii) Demonstrated expertise in responding to incidents involving weapons of mass destruction and biological warfare.
(iii) Demonstrated expertise in emergency medical services.
(iv) Demonstrated expertise in chemical, biological, radiological, and nuclear countermeasures.
(v) Strong affiliations with animal and plant diagnostic laboratories.
(vi) Demonstrated expertise in food safety.
(vii) Affiliation with Department of Agriculture laboratories or training centers.
(viii) Demonstrated expertise in water and wastewater operations.
(ix) Demonstrated expertise in port and waterway security.
(x) Demonstrated expertise in multi-modal transportation.
(xi) Nationally recognized programs in information security.
(xii) Nationally recognized programs in engineering.
(xiii) Demonstrated expertise in educational outreach and technical assistance.
(xiv) Demonstrated expertise in border transportation and security.
(xv) Demonstrated expertise in interdisciplinary public policy research and communication outreach regarding science, technology, and public policy.
(C) DISCRETION OF SECRETARY.—The Secretary shall have the discretion to establish such centers and to consider additional criteria as necessary to meet the evolving needs of homeland security and shall report to Congress concerning the implementation of this paragraph as necessary.
(D) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as may be necessary to carry out this paragraph.
(c) INTRAMURAL PROGRAMS.—

(1) CONSULTATION.—In carrying out the duties under section 302, the Secretary, acting through the Under Secretary for Science and Technology, may draw upon the expertise of any laboratory of the Federal Government, whether operated by a contractor or the Government.
(2) LABORATORIES.—The Secretary, acting through the Under Secretary for Science and Technology, may establish a headquarters laboratory for the Department at any laboratory or site and may establish additional laboratory units at other laboratories or sites.
(3) CRITERIA FOR HEADQUARTERS LABORATORY.—If the Secretary chooses to establish a headquarters laboratory pursuant to paragraph (2), then the Secretary shall do the following:
(A) Establish criteria for the selection of the headquarters laboratory in consultation with the National Academy of Sciences, appropriate Federal agencies, and other experts.
(B) Publish the criteria in the Federal Register.
(C) Evaluate all appropriate laboratories or sites against the criteria.
(D) Select a laboratory or site on the basis of the criteria.
(E) Report to the appropriate congressional committees on which laboratory was selected, how the selected laboratory meets the published criteria, and what duties the headquarters laboratory shall perform.
(4) LIMITATION ON OPERATION OF LABORATORIES.—No laboratory shall begin operating as the headquarters laboratory of the Department until at least 30 days after the transmittal of the report required by paragraph (3)(E).

SEC. 309. UTILIZATION OF DEPARTMENT OF ENERGY NATIONAL LABORATORIES AND SITES IN SUPPORT OF HOMELAND SECURITY ACTIVITIES.
(a) AUTHORITY TO UTILIZE NATIONAL LABORATORIES AND SITES.—
(1) IN GENERAL.—In carrying out the missions of the Department, the Secretary may utilize the Department of Energy national laboratories and sites through any 1 or more of the following methods, as the Secretary considers appropriate:
(A) A joint sponsorship arrangement referred to in subsection (b).
(B) A direct contract between the Department and the applicable Department of Energy laboratory or site, subject to subsection (c).
(C) Any ''work for others'' basis made available by that laboratory or site.
(D) Any other method provided by law.
(2) ACCEPTANCE AND PERFORMANCE BY LABS AND SITES.—
Notwithstanding any other law governing the administration, mission, use, or operations of any of the Department of Energy national laboratories and sites, such laboratories and sites are authorized to accept and perform work for the Secretary, consistent with resources provided, and perform such work on an equal basis to other missions at the laboratory and not on a noninterference basis with other missions of such laboratory or site.
(b) JOINT SPONSORSHIP ARRANGEMENTS.—
(1) LABORATORIES.—The Department may be a joint sponsor, under a multiple agency sponsorship arrangement with the Department of Energy, of 1 or more Department of Energy national laboratories in the performance of work.
(2) SITES.—The Department may be a joint sponsor of a Department of Energy site in the performance of work as if such site were a federally funded research and development center and the work were performed under a multiple agency sponsorship arrangement with the Department.
(3) PRIMARY SPONSOR.—The Department of Energy shall be the primary sponsor under a multiple agency sponsorship arrangement referred to in paragraph (1) or (2).
(4) LEAD AGENT.—The Secretary of Energy shall act as the lead agent in coordinating the formation and performance of a joint sponsorship arrangement under this subsection between the Department and a Department of Energy national laboratory or site.

(5) FEDERAL ACQUISITION REGULATION.—Any work performed by a Department of Energy national laboratory or site under a joint sponsorship arrangement under this subsection shall comply with the policy on the use of federally funded research and development centers under the Federal Acquisition Regulations.
(6) FUNDING.—The Department shall provide funds for work at the Department of Energy national laboratories or sites, as the case may be, under a joint sponsorship arrangement under this subsection under the same terms and conditions as apply to the primary sponsor of such national laboratory under section 303(b)(1)(C) of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 253(b)(1)(C)) or of such site to the extent such section applies to such site as a federally funded research and development center by reason of this subsection.
(c) SEPARATE CONTRACTING.—To the extent that programs or activities transferred by this Act from the Department of Energy to the Department of Homeland Security are being carried out through direct contracts with the operator of a national laboratory or site of the Department of Energy, the Secretary of Homeland Security and the Secretary of Energy shall ensure that direct contracts for such programs and activities between the Department of Homeland Security and such operator are separate from the direct contracts of the Department of Energy with such operator.
(d) AUTHORITY WITH RESPECT TO COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENTS AND LICENSING AGREEMENTS.—In connection with any utilization of the Department of Energy national laboratories and sites under this section, the Secretary may permit the director of any such national laboratory or site to enter into cooperative research and development agreements or to negotiate licensing agreements with any person, any agency or instrumentality, of the United States, any unit of State or local government, and any other entity under the authority granted by section 12 of the Stevenson-Wydler Technology Innovation Act
of 1980 (15 U.S.C. 3710a). Technology may be transferred to a non-Federal party to such an agreement consistent with the provisions of sections 11 and 12 of that Act (15 U.S.C. 3710, 3710a).
(e) REIMBURSEMENT OF COSTS.—In the case of an activity carried out by the operator of a Department of Energy national laboratory or site in connection with any utilization of such a laboratory or site under this section, the Department of Homeland Security shall reimburse the Department of Energy for costs of such activity through a method under which the Secretary of Energy waives any requirement for the Department of Homeland Security to pay administrative charges or personnel costs of the Department of Energy or its contractors in excess of the amount that the Secretary of Energy pays for an activity carried out by such contractor and paid for by the Department of Energy.
(f) LABORATORY DIRECTED RESEARCH AND DEVELOPMENT BY THE DEPARTMENT OF ENERGY.—No funds authorized to be appropriated or otherwise made available to the Department in any fiscal year may be obligated or expended for laboratory directed research and development activities carried out by the Department of Energy unless such activities support the missions of the Department of Homeland Security.
(g) OFFICE FOR NATIONAL LABORATORIES.—There is established within the Directorate of Science and Technology an Office for National Laboratories, which shall be responsible for the coordination and utilization of the Department of Energy national laboratories and sites under this section in a manner to create a networked laboratory system for the purpose of supporting the missions of the Department.
(h) DEPARTMENT OF ENERGY COORDINATION ON HOMELAND SECURITY RELATED RESEARCH.—The Secretary of Energy shall ensure that any research, development, test, and evaluation activities conducted within the Department of Energy that are directly or indirectly related to homeland security are fully coordinated with the Secretary to minimize duplication of effort and maximize the effective application of Federal budget resources.

SEC. 310. TRANSFER OF PLUM ISLAND ANIMAL DISEASE CENTER, DEPARTMENT OF AGRICULTURE.
(a) IN GENERAL.—In accordance with title XV, the Secretary of Agriculture shall transfer to the Secretary of Homeland Security the Plum Island Animal Disease Center of the Department of Agriculture, including the assets and liabilities of the Center.

(b) CONTINUED DEPARTMENT OF AGRICULTURE ACCESS.—On completion of the transfer of the Plum Island Animal Disease Center under subsection (a), the Secretary of Homeland Security and the Secretary of Agriculture shall enter into an agreement to ensure that the Department of Agriculture is able to carry out research, diagnostic, and other activities of the Department of Agriculture at the Center.
(c) DIRECTION OF ACTIVITIES.—The Secretary of Agriculture shall continue to direct the research, diagnostic, and other activities of the Department of Agriculture at the Center described in subsection (b).
(d) NOTIFICATION.—
(1) IN GENERAL.—At least 180 days before any change in the biosafety level at the Plum Island Animal Disease Center, the President shall notify Congress of the change and describe the reasons for the change.
(2) LIMITATION.—No change described in paragraph (1) may be made earlier than 180 days after the completion of the transition period (as defined in section 1501).

SEC. 311. HOMELAND SECURITY SCIENCE AND TECHNOLOGY ADVISORY COMMITTEE.
(a) ESTABLISHMENT.—There is established within the Department a Homeland Security Science and Technology Advisory Committee (in this section referred to as the ''Advisory Committee''). The Advisory Committee shall make recommendations with respect to the activities of the Under Secretary for Science and Technology, including identifying research areas of potential importance to the security of the Nation.
(b) MEMBERSHIP.—
(1) APPOINTMENT.—The Advisory Committee shall consist of 20 members appointed by the Under Secretary for Science and Technology, which shall include emergency first-responders
or representatives of organizations or associations of emergency first-responders. The Advisory Committee shall also include representatives of citizen groups, including economically disadvantaged communities. The individuals appointed as members of the Advisory Committee—
(A) shall be eminent in fields such as emergency response, research, engineering, new product development, business, and management consulting;
(B) shall be selected solely on the basis of established records of distinguished service;
(C) shall not be employees of the Federal Government; and
(D) shall be so selected as to provide representation of a cross-section of the research, development, demonstration, and deployment activities supported by the Under Secretary for Science and Technology.
(2) NATIONAL RESEARCH COUNCIL.—The Under Secretary for Science and Technology may enter into an arrangement for the National Research Council to select members of the
Advisory Committee, but only if the panel used by the National Research Council reflects the representation described in paragraph (1).
(c) TERMS OF OFFICE.—
(1) IN GENERAL.—Except as otherwise provided in this subsection, the term of office of each member of the Advisory Committee shall be 3 years.
(2) ORIGINAL APPOINTMENTS.—The original members of the Advisory Committee shall be appointed to three classes of three members each. One class shall have a term of 1 year, 1 a term of 2 years, and the other a term of 3 years.
(3) VACANCIES.—A member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed for the remainder of such term.
(d) ELIGIBILITY.—A person who has completed two consecutive full terms of service on the Advisory Committee shall thereafter be ineligible for appointment during the 1-year period following the expiration of the second such term.
(e) MEETINGS.—The Advisory Committee shall meet at least quarterly at the call of the Chair or whenever one-third of the members so request in writing. Each member shall be given appropriate notice of the call of each meeting, whenever possible not less than 15 days before the meeting.
(f) QUORUM.—A majority of the members of the Advisory Committee not having a conflict of interest in the matter being considered by the Advisory Committee shall constitute a quorum.

(g) CONFLICT OF INTEREST RULES.—The Advisory Committee shall establish rules for determining when 1 of its members has a conflict of interest in a matter being considered by the Advisory Committee.
(h) REPORTS.—
(1) ANNUAL REPORT.—The Advisory Committee shall render an annual report to the Under Secretary for Science and Technology for transmittal to Congress on or before January 31 of each year. Such report shall describe the activities and recommendations of the Advisory Committee during the previous year.
(2) ADDITIONAL REPORTS.—The Advisory Committee may render to the Under Secretary for transmittal to Congress such additional reports on specific policy matters as it considers appropriate.
(i) FEDERAL ADVISORY COMMITTEE ACT EXEMPTION.—Section 14 of the Federal Advisory Committee Act shall not apply to the Advisory Committee.
(j) TERMINATION.—The Department of Homeland Security Science and Technology Advisory Committee shall terminate 3 years after the effective date of this Act.

SEC. 312. HOMELAND SECURITY INSTITUTE.
(a) ESTABLISHMENT.—The Secretary shall establish a federally funded research and development center to be known as the ''Homeland Security Institute'' (in this section referred to as the ''Institute'').
(b) ADMINISTRATION.—The Institute shall be administered as a separate entity by the Secretary.
(c) DUTIES.—The duties of the Institute shall be determined by the Secretary, and may include the following:
(1) Systems analysis, risk analysis, and simulation and modeling to determine the vulnerabilities of the Nation's critical infrastructures and the effectiveness of the systems deployed to reduce those vulnerabilities.
(2) Economic and policy analysis to assess the distributed costs and benefits of alternative approaches to enhancing security.
(3) Evaluation of the effectiveness of measures deployed to enhance the security of institutions, facilities, and infrastructure that may be terrorist targets.
(4) Identification of instances when common standards and protocols could improve the interoperability and effective utilization of tools developed for field operators and first responders.
(5) Assistance for Federal agencies and departments in establishing testbeds to evaluate the effectiveness of technologies under development and to assess the appropriateness of such technologies for deployment.
(6) Design of metrics and use of those metrics to evaluate the effectiveness of homeland security programs throughout the Federal Government, including all national laboratories.
(7) Design of and support for the conduct of homeland security-related exercises and simulations.
(8) Creation of strategic technology development plans to reduce vulnerabilities in the Nation's critical infrastructure and key resources.
(d) CONSULTATION ON INSTITUTE ACTIVITIES.—In carrying out the duties described in subsection (c), the Institute shall consult widely with representatives from private industry, institutions of higher education, nonprofit institutions, other Government agencies, and federally funded research and development centers.
(e) USE OF CENTERS.—The Institute shall utilize the capabilities of the National Infrastructure Simulation and Analysis Center.
(f) ANNUAL REPORTS.—The Institute shall transmit to the Secretary and Congress an annual report on the activities of the Institute under this section.
(g) TERMINATION.—The Homeland Security Institute shall terminate 3 years after the effective date of this Act.

SEC. 313. TECHNOLOGY CLEARINGHOUSE TO ENCOURAGE AND SUPPORT INNOVATIVE SOLUTIONS TO ENHANCE HOMELAND SECURITY.
(a) ESTABLISHMENT OF PROGRAM.—The Secretary, acting through the Under Secretary for Science and Technology, shall establish and promote a program to encourage technological innovation in facilitating the mission of the Department (as described in section 101).

(b) ELEMENTS OF PROGRAM.—The program described in subsection (a) shall include the following components:
(1) The establishment of a centralized Federal clearinghouse for information relating to technologies that would further the mission of the Department for dissemination, as appropriate,
to Federal, State, and local government and private sector entities for additional review, purchase, or use.
(2) The issuance of announcements seeking unique and innovative technologies to advance the mission of the Department.
(3) The establishment of a technical assistance team to assist in screening, as appropriate, proposals submitted to the Secretary (except as provided in subsection (c)(2)) to assess the feasibility, scientific and technical merits, and estimated cost of such proposals, as appropriate.
(4) The provision of guidance, recommendations, and technical assistance, as appropriate, to assist Federal, State, and local government and private sector efforts to evaluate and implement the use of technologies described in paragraph (1) or (2).
(5) The provision of information for persons seeking guidance on how to pursue proposals to develop or deploy technologies that would enhance homeland security, including information relating to Federal funding, regulation, or acquisition.
(c) MISCELLANEOUS PROVISIONS.—
(1) IN GENERAL.—Nothing in this section shall be construed as authorizing the Secretary or the technical assistance team established under subsection (b)(3) to set standards for technology
to be used by the Department, any other executive agency, any State or local government entity, or any private sector entity.
(2) CERTAIN PROPOSALS.—The technical assistance team established under subsection (b)(3) shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.
(3) COORDINATION.—In carrying out this section, the Secretary shall coordinate with the Technical Support Working Group (organized under the April 1982 National Security Decision
Directive Numbered 30).