Privacy Impact Assessment Update
for the
Standoff Technology Integration and Demonstration Program

October 14, 2010

Contact Point

Joe Foster

Program Manager, Explosives Division

Science and Technology Directorate

202-254-5314

Reviewing Official

Mary Ellen Callahan

Chief Privacy Officer

Department of Homeland Security

703-235-0780

Abstract

The U.S. Department of Homeland Security's (DHS's) Science and Technology Directorate (S&T) is updating the Standoff Explosives Detection Technology Demonstration Program (now referred to as the Standoff Technology Integration and Demonstration Program, or STIDP) Privacy Impact Assessment (PIA) issued July 21, 2008 to reflect updates to the program involving live crowd testing.

The program is adding new technologies, expanding the use of the test center, enhancing object tracking technologies and beginning to distribute crowd video data to vendors. This PIA update identifies and addresses the privacy issues associated with public test and evaluation activities on technologies that will be acquired, matured, and integrated by STIDP between now and the end of the program, currently slated for 2014. Based on the privacy issues identified, three sets of privacy protective requirements were developed and implemented at all stages of the program. The Live Testing Requirements and Law Enforcement Operations Requirements apply to conducting and operating a test in a public environment and the Data Protection Requirements[1] address the collection and protection of personally identifiable information (PII). These requirements, when systematically applied to test and evaluation plans and their implementation, ensure that privacy concerns are appropriately addressed for broad classes of technologies tested in a range of venues with and without law enforcement operations. This update assists STIDP's mission of developing an integrated countermeasure architecture to prevent person-borne improvised explosive device attacks.

Introduction

STIDP is updating its PIA because of the addition of new first-line sensors, an expansion of the use of the Toyota Center, an enhancement of the object tracking technology, and distribution of crowd video data to vendors.

STIDP Mission and Technical Approach

Moving crowds such as patrons approaching large public events, make attractive targets for terrorists. DHS and the Department of Defense (DoD) co-fund the Standoff Technology Integration and Demonstration Program, or STIDP, to detect and counter improvised explosive devices (IEDs) in crowd environments. The intent is to find and intercept person-borne improvised explosive devices (PBIEDs) at a distance (i.e., standoff detection) before detonation can occur, thus protecting people, property, and critical infrastructure.

In most counter-IED approaches used today, operators make interdiction decisions based on individual data sources, such as concealed object detection sensors or suspicious behavior surveillance. STIDP's next-generation approach improves decision-making using a highly automated system that integrates detection systems and prioritizes threats—without impeding crowd flow. Operators then can mobilize assets to target the highest potential risks.

[1] See Section titled "Summary of STIDP Privacy Approach"

The conceptual PBIED architecture is the framework on which the STIPD program operates. The architecture is a layered set of countermeasures integrated and operated as a system via a suite of enabling technologies and a unified concept of operations. First-line sensors triage the arriving crowd, identifying people of interest who should be interrogated with one or more screening technologies. People are tracked and their coordinates are passed to a system that prioritizes screening based on rules. The system then transmits coordinates to the appropriate downstream sensor and a scan is conducted. The screening result is displayed to the operator and associated data are captured for operator examination, if necessary. The process continues until all the people in the screening zone are screened.

STIDP uses an iterative development approach that involves identifying commercially available technical solutions; modifying or maturing them to meet the architecture requirements of screening a crowd, integrating the solutions, testing them in controlled and live crowd environments, and providing feedback to technology developers. Lessons learned drive the evolution of the integrated countermeasure architecture. Capability gaps in countermeasure and enabling technologies are identified as areas of research and development.

Test and Evaluation Methodology

Substantial technical challenges remain with respect to the goal of a risk-based, automated screening system for crowds. First-line sensors capable of triaging the arriving crowd must overcome line-of-sight issues and provide coverage over large entrance areas. Because of these challenges, STIDP will conduct routine test and evaluation of stand-alone modules and of the integrated countermeasure system to learn about its capabilities and limitations.

Standalone and integrated system controlled and live testing at the Toyota Center will be conducted as necessary to assess the technology at various stages of its development. Controlled testing will be done with Pacific Northwest National Laboratory (PNNL) staff or volunteers under known and controlled conditions. Volunteers to support testing will be required to sign informed consent forms giving permission to use their images for R&D purposes. Live testing with crowds will be conducted when there is sufficient confidence in the technology/system to address the unknown and unexpected clutter from a live environment. During both tests, surveillance cameras and various sensors may capture video images of individuals. Live crowd testing will be far less frequent than controlled testing. The uncontrolled nature of these tests will provide valuable insights into a technology's performance in an operational environment.

Throughout the analysis, three classes of privacy protection requirements have been defined for testing activities that involve live crowds: Live Event Requirements (providing notification and an alternative, opt-out entrance for the public), Data Protection Requirements (controlling the collection, protection, and transmission of PII), and Law Enforcement Operations Requirements (addressing the interdiction of the public). These requirements are applied consistently throughout the various stages of testing activities documented in this PIA, and are described in further detail below:

- **Live Testing Requirements:** When conducting tests that involve the collection of PII and video/sensor images from members of the public, signage will be posted informing the public of the testing activities. Additionally an alternative opt-out entrance will be provided to those who wish not to participate in the testing activities. These activities may include the testing of stand-

alone modules (e.g., first-line or standoff sensors), integrated modules, or the collection of crowd video data. This requirement is consistent with the original PIA.

- **Law Enforcement Operations Requirements:** If testing includes interdiction of the public based on a sensor response, interdiction will only be conducted by participating law enforcement entities or local security personnel in accordance with their local authority and standard operating procedures. This requirement is consistent with the original PIA.
- **Data Protection Requirements:** Data containing PII and video images collected by STIDP will be protected as described below to prevent the unauthorized access to or use of the information, and retention of more information than is otherwise necessary. With the exception of the retention period and the expansion of data sharing to non-STIDP vendors, these requirements are consistent with the original PIA.

    1. Data will be available only to organizations and individuals with a valid need to know.
    2. Data will be stored on password protected systems in secure facilities.
    3. Transmission of data will be encrypted and/or password protected.
    4. Upon termination of the project, all data that had been collected will be destroyed.
    5. PNNL's approval process will ensure compliance with this PIA and the requirement that identifiable faces must be blurred. If data is needed for client, vendor, stakeholder, industry, academia, interactions where an electronic or printed image is required, the data to be released will be approved in advance by PNNL.
    6. Data shared with STIDP vendors and object tracking developers will be on a need to know basis and will be required to sign a non-disclosure agreement (NDA) legally committing their compliance to the terms and conditions of this PIA. Companies that receive object tracking data sets must be approved in advance by PNNL. The NDA will require compliance with items 1-5 above.
    7. Companies accessing the test bed and collecting PII data on their system will be required to sign an NDA legally committing their compliance to the terms and conditions of this PIA. The NDA will require compliance with items 1-5 above.

Live Crowd Testing

Testing with live crowds can occur in different ways. Tests could support the evaluation of individual modules such as magnetometers or in support of multiple technologies as part of an integrated countermeasure system. Test operations with/without law enforcement actions with live crowds can occur in any of the three scenarios described below:

1. PNNL researchers may operate the technologies with a live crowd, observing the response of a sensor or sensor systems to arriving patron traffic. Data from the sensors would be collected and analyzed, but no law enforcement action would take place (e.g., interdiction). *Under no conditions will PNNL or its contractors perform law enforcement actions.*

2. Law enforcement or security personnel would operate the technologies with a live crowd. Law enforcement or security personnel represent potential end users of the technology; as such, feedback from this group is important relative to the design of the system. Data from the sensors would be collected, but no law enforcement action would take place (e.g., interdiction). Information on the sensor performance would be obtained as well as operator input on the system itself (e.g., usability, human-system interface design).
3. Law enforcement or security personnel would operate the technologies with a live crowd. Data from the sensors would be collected and law enforcement action (e.g., interdiction) could take place based on one or more sensor alerts. Any interdictions would be consistent with the Law Enforcement Operating Requirements. These requirements state that interdictions are to be conducted only by local law enforcement or security personnel based on local laws and standard operating procedures. These requirements are originally defined and approved in the initial PIA.

Collection of Personally Identifiable Information

There are a number of architecture modules that collect PII when tested in public venues due to their use of video cameras. While the resolution of the captured images may not produce identifiable images, it is assumed for the purposes of this PIA that all images collected are PII. The modules that collect PII include:

- **Standoff detection sensors**: Irrespective of whether the raw or processed sensor output contains PII or not, these sensors routinely include video cameras so that the person of interest being scanned is known to the operators. Thus, for purposes of this PIA, standoff detection sensors are assumed to generate PII. The range of standoff sensors that could be integrated into the STIDP architecture as defined in the initial PIA is provided in Appendix A; the set of sensors added via this PIA update are presented in Appendix B.
- **First-line sensors**: Although current first-line sensor concepts do not generate PII, first-line sensors may include the use of video cameras. Thus, for purposes of this PIA, standoff detection sensors are assumed to generate PII.
- **Surveillance cameras:** They are used to provide operator situational awareness, to support test and evaluation activities (including post-test analyses), and to support the advancement of key modules such as object tracking.
- **Object tracking cameras:** They collect raw video for processing by software to identify and track objects of interest.

Additional information on each technology will be provided later in the PIA. Any data generated or collected by these systems will be protected according to the Data Protection Requirements.

Background

On July 21, 2008, S&T issued a PIA to document the STIDP, a multiyear research, development, testing, and evaluation (RDT&E) program designed to facilitate the development of an integrated countermeasure architecture to prevent person-borne improvised explosive attacks in crowd

environments. As described in that PIA, S&T continues to fund PNNL and to work with other partnering entities, including DoD, to conduct this RDT&E program.[2]

The initial PIA addressed:

- specific standoff detection technologies (infrared cameras and millimeter wave radar technologies to detect concealed objects) and video analytics technology (for anomaly detection and object tracking of live crowds) that were deployed and integrated as a system and tested in a public environment;
- identification of standoff detection technologies of interest to DHS S&T;
- requirements for the interdiction of arriving patrons by law enforcement officers based on the sensor data captured by standoff sensors;
- the use of surveillance cameras to provide situational awareness for the operators and an image feed for video analytics software;
- requirements for live testing, including the use of signs notifying the public of testing and an opt-out; and
- requirements to protect PII information and prevent its unintentional release.

In the fall of 2008, STIDP carried out a series of tests at the Toyota Center in Kennewick, WA. Initial scoping tests were conducted to evaluate the performance of the deployed technologies in their new environment and controlled characterization tests were conducted to establish a baseline of the technology and system performance. Both the scoping and controlled characterization tests were conducted with volunteers and without the presence of a live crowd. Law enforcement personnel were trained as operators for these tests and the tests with live crowds. Five tests were conducted with live crowds. Notice was provided during the live crowd testing.

The live field tests were very successful; STIDP's programmatic test objectives were achieved. The vendors learned firsthand about the gaps in their technologies; testing insights led to new architecture concepts better suited for live crowds and the stakeholders' (e.g., venue owner/operator, and the public) experiences were extremely positive. The imaging and standoff sensors technologies deployed for these tests have since been removed from the site with the exception of three surveillance cameras.

Following the initial field tests, STIDP worked with the venue owner and operator to create the Standoff Detection Test Bed, a unique asset where testing and evaluation of sensors and other key counter-IED technologies can be assessed in a live crowd environment. This PIA update describes the delivery of this capability to DHS, DoD, and their partners.

[2] The initial PIA for this, Standoff Explosives Detection Technology Demonstration Program, published on July 21, 2008, can be found at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_sodtp.pdf.

Reason for Update

S&T is updating the STIDP PIA issued July 21, 2008 to reflect the following changes to the program execution:

1. the addition of first-line sensors, such as magnetometers to the suite of countermeasure technologies being tested;
2. updates to the original table of approved standoff detection technologies (Appendix A) to reflect a wider range of technologies (Appendix B);
3. expansion of the use of the Toyota Center in Kennewick, WA to other government agencies and relevant industry;
4. expansion of STIDP test venues beyond the Toyota Center to enhance object tracking technologies and provide alternative, representative testing environments for the integrated PBIED countermeasures;
5. distribution of crowd video data to vendors and the research and development (R&D) community involved in developing and assessing object tracking architectures and algorithms; and
6. expanded retention of data (until program closeout in 2014) to enable researchers to continue to develop and evaluate technical solutions over multiple generations.

1. First-line Sensors

This update discusses first-line sensors and how they may be involved in the generation of PII.

To address the need to triage the arriving crowd, the researchers envision deploying a suite of first-line sensors. First-line sensors will act as a trip line to trigger the rest of the standoff system to focus on potential anomalies (i.e., an individual carrying a large amount of metal). First-line sensors are differentiated from standoff sensors due to their function in the overall integrated PBIED architecture and potentially different operating principles. For example, the first-line sensors scan a designated area while the standoff sensors scan individuals. One desirable feature of a first-line sensor is that it is not affected by line-of-sight issues that may occur with crowd flow.

The added technologies include:

- Magnetometers; and
- Electronic nose technologies.

PNNL is evaluating commercial-off-the-shelf (COTS) and near-COTS first-line technologies in phases through a series of standalone tests using members of the research team as volunteers, volunteers to simulate crowd environments, and eventually using live crowds. The conduct of live tests of first-line sensor systems is defined by the Live Testing Requirements and Law Enforcement Operations Requirements; the protection of PII data is defined by the Data Protection Requirements. Relative to venue operations, these requirements mean that signage will be posted notifying the public of the testing activities and an alternative opt-out entrance will be provided. If law enforcement or local security

personnel are participating in the activities, they will conduct interdictions in accordance to their own regulations and standard operating procedures.

If the initial test results indicate that the technology is viable, testing will be conducted with live crowds. Further investments may be made to increase sensitivity, improve its ability to discriminate threats from non-threats, and improve deployability (e.g., reduce size, power requirements). Once completed, another round of controlled and live tests would be conducted

Magnetometers and electronic nose technologies are passive sensors that can detect changes in the local magnetic field or the presence of explosive chemicals. They are area sensors (e.g., they can detect the presence of metal or explosive compounds within its sensing radius); they do not capture imagery or any other identifying information and require no direct interaction with the individual. In the event of a detection, the magnetometers and electronic nose will signal that something has been detected. Signals are typically an indicator on an operator's screen (e.g., light going off or an alarm sounds off).

Regardless of whether the first-line sensor collects PII or not, video cameras will typically be deployed with first-line sensors for situational awareness (how many people and what objects are in the vicinity of the sensor) and post-test analysis.

2. Standoff Technologies

This update addresses the expansion of standoff technologies covered under the original PIA.

The original PIA documented the testing and evaluation of passive and active millimeter wave (MMW) imaging and sensor technologies. PNNL will continue to consider MMW technologies for the overall integrated countermeasure system of systems. This PIA update will add to the list of approved standoff sensor and imaging technologies to include a wider range of such technologies.

The added technologies include:

- passive and active submillimeter wave (SMMW);
- terahertz (THz) imaging and sensor technologies; and
- acoustic sensor and imaging technologies.

These additional technologies operate in an identical manner to the previously approved MMW technologies; the only difference is the portion of the reflected electromagnetic spectrum that is captured (e.g., different wavelengths) to detect an anomaly on a person.

The MMW, SMMW, and THz technologies work by sensing the reflected energy from a person in the corresponding wavelength. Person-carried objects change how the energy is reflected, resulting in an unusual return signal or image. The image-generating technologies that operate in these wavelengths do not produce an identifiable image, the same way that a picture of a person in the infrared spectrum does not provide PII. Acoustic imaging and sensor technologies, rather than detecting light, detect the reflection of ultrasound waves. As with the above mentioned technologies, the image generated acoustically does not produce PII.

The SMMW and THz imaging technologies may produce a clearer (less grainy) image than the original MMW technology. However, as described in the original PIA, these technologies alone cannot

produce identifiable images of an individual. Because these sensors integrate a video camera into their system so that a person of interest can be identified, PII is expected to be generated when these sensors are used in a live crowd environment.

The conduct of live tests of these standoff detection systems is defined by the Live Testing Requirements and Law Enforcement Operations Requirements; the protection of PII data is defined by the Data Protection Requirements.

3. Expanded Use of the Toyota Center for Evaluation of Technologies

This update discusses the expanded use of the Toyota Center for the test and evaluation of technologies under development by other government agencies and industry.

The initial use of the Toyota Center involved integrating and conducting tests on technologies developed or acquired by PNNL under contract to support the initial STIDP test objectives. The success of the fiscal year 2008 field demonstrations, the long-term testing needs of DHS and DoD, and the need to expose a broader range of industry-developed technologies to live crowd environments led to STIDP creating the Standoff Detection Test Bed at the Toyota Center (SDTB).

The use of the SDTB will expand beyond technologies developed by PNNL and its vendors to technologies being developed by other government agencies as well as those under development by relevant industry. Testing will include stand-alone testing of key modules provided by other government agencies or industry and the potential integration of those technologies into STIDP's PBIED architecture under both controlled and live crowd conditions.

Procedures have been developed for how PNNL will evaluate candidates for using the Test Bed. PNNL will ensure that they conform to all PNNL security and environmental safety and health issues, and conform to the privacy protections outlined in this PIA. PNNL will manage all access to the SDTB and the collection and destruction of data.

Organizations that are approved to use the test bed will conduct controlled tests using volunteers and/or with live crowds. In a live crowd setting, it is likely that the vendors will more than likely collect PII data on their systems (e.g., standoff sensors employing video cameras, object tracking system).

The Live Testing Requirements and Data Protection Requirements defined below will apply when any tests are conducted with live crowds. If law enforcement operations are required, Law Enforcement Operations Requirements will apply.

4. Expansion to Other Venues

This update discusses the expansion of testing to other venues. The expansion will include capturing diverse crowd video data sets and testing of STIDP integrated technologies at diverse representative venues.

To evaluate vendors' capabilities and to advance the technology, a more expansive library of video data sets of large, unstructured crowds is needed to test object tracking algorithms. Because the Toyota Center is a relatively small venue with a relatively simple footprint, diverse crowd video data at larger, more complex venues is needed for sound and rapid progress to be made on object tracking system and algorithm design.

While there are several technical approaches for tracking human targets over distance, video analytics-based tracking algorithms best addresses the technical and operational requirements defined by STIDP. Video from one or more cameras are analyzed by software; human-like objects are identified (vs. cars, flagpoles) and those objects are tracked by a variety of algorithms (e.g., pattern recognition). One advantage of video-based methods is that they can also detect anomalies such as loitering individuals.

Object tracking requirements are quite challenging, with the main need to track large numbers of persons across multiple cameras in all types of environmental conditions (including low light) with high tracking fidelity and accurate coordinate generation. The spatial coordinates of individuals of interest being tracked are provided to a command and control system that then directs a standoff sensor to obtain a scan of that person. Using this approach, the operator is freed up from tedious positioning of sensors and can focus on managing overall risk of the screening process.

Collection of Crowd Video Data Sets at Other Venues

PNNL will consult an advisory group consisting of key industry segments (National Football League, Major League Baseball) on potential venues that might offer representative crowd flows and will help STIPD acquire the necessary video data.

The use of video cameras for the project was approved in the original PIA.

Testing and Evaluation of the PBIED Integrated Architecture at Other Venues

While the Toyota Center provides representative crowd dynamics of larger venues, there may be technical drivers to conduct live testing of an integrated set of technologies at a larger, more challenging and representative venue. DHS has had and continues to have discussions with sports stadiums regarding a potential demonstration of STIDP integrated technologies. Because of the varying nature of potential deployment scenarios other testing venues may be needed.

Regardless of where technologies are tested in a live environment by STIDP, the Live Testing Requirement and Data Protection Requirements would apply. The Law Enforcement Requirement will be levied when law enforcement or security personnel serve as operators.

5. Distribution of Video Data Sets beyond STIDP Vendors

While the STIDP vendor will have access to the video data sets collected at the additional venues (in addition to the Toyota Center), there is a need to advance the object tracking community's capabilities so that ultimately, a solution that meets STIDPs needs can be provided, recognizing that the better solutions may come from outside of a single vendor. To drive research and development efforts of the object tracking community, PNNL will provide these video data sets to qualified developers outside the STIDP research team that are willing to make internal investments (e.g., labor) in assessing and further developing their object tracking algorithms/systems. Because of the internal costs involved, a relatively few number of players in the community are expected to request the data sets. Note that the data sets offer the opportunity not just to test and evaluate algorithms, but also the overall object tracking system design (where and how processing is done, e.g. at the camera and/or workstation).

The Data Protection Requirements will apply to the protection, transfer, and release of object tracking video data sets.

6. Extension of the Retention Period for the Data

In the original PIA, a 90-day period was estimated to be sufficient to perform analyses of the video and other data captured during the controlled and live tests. However, the program team has now determined that additional time is necessary to thoroughly analyze the data and present the results to DHS and DoD and other key stakeholders. More importantly, the utility of the live crowd video sets is much greater than that of the controlled test data given that the live data sets can be used to evaluate multiple generations of algorithm and architecture approaches (e.g., types of cameras, computational approaches to processing information, network design). Because of these reasons, the data retention period is extended to the conclusion of the program, now scheduled for 2014 (subject to change). The retention period is defined as part of the Data Protection Requirements.

Privacy Impact Analysis

Each of the following sections consider how the system has changed and what impact it has on the below fair information principles. In some cases, there may be no changes and this is indicated.

The System and the Information Collected and Stored Within the System

STIDP is developing a suite of systems to deliver an integrated set of layered countermeasures to prevent suicide bomber attacks. The original PIA addressed the collection of PII generated by a system consisting of 1) surveillance cameras, 2) standoff detection systems 3) video analytics cameras. The results from initial testing using this integrated set of countermeasures highlighted the shortcomings of the sensor systems and how they were integrated and operated as a system. These shortcomings are being addressed by STIDP and via this PIA.

Going forward, the following modules are expected to generate PII: surveillance cameras, standoff sensors, first-line sensors, and object tracking systems. When testing as an integrated system, data is typically collected at the module and system level. If PII is captured at the module level, then the system level data is defined as PII data as well. In both cases, the Data Protection Requirements apply.

PNNL will test the modules in a controlled environment using volunteers from the research team, as well as with live crowds. Should the system being developed require testing with a live crowd, the Live Event Requirement will be applied, including posting signage notifying the public of the collection of video data. Depending on the testing scenario, the tests may include law enforcement personnel as operators. The Law Enforcement Requirement will be levied when law enforcement or security personnel serve as operators and interact with the public. All interdiction or law enforcement activities will be conducted in accordance to applicable standard operating procedures.

Uses of the System and the Information

The use of the information collected by the system during the program remains the same as documented in the original PIA: test and evaluate an integrated set of countermeasures for preventing PBIED attacks in crowd environments. If successful, the system may be deployed as part of a venue's

security measures or as an enhanced security feature for protecting forward operating bases, marketplaces. This PIA will only cover the privacy issues associated with the RDT&E activities; any additional analysis of the privacy issues associated with deploying the system in an operational setting will be conducted by the end user.

The information generated by the system will be used to baseline technology performance as well as identify gaps in performance at the module or system level. The gaps will help drive public and private investments to overcome limitations in performance. PNNL will also produce a final report on the utility of the modules and technologies at the conclusion of the program.

Vendors under contract to PNNL will be provided module and where appropriate, system level data and an assessment of how their systems performed. Industrial and other government agency users of the test bed will receive data reports on their technologies performance. Members of the object tracking community will be eligible to receive data to benchmark and drive the development of their systems. Data Protection Requirements have been defined to protect and prevent the inadvertent release of PII data transmitted to third parties. Non Disclosure Agreements (NDAs), required prior to receiving any data, are the foundation of the data protection strategy by binding the signatory to the multiple data protection requirements.

Retention

General Records System 20, Item 1 will still cover the disposition of electronic files or records created solely to test system performance, as well as hard-copy print-outs and related documentation for electronic files/records. According to General Records System 20, records should be "delete[d]/destroy[ed] when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes." In the original PIA, the program team determined that 90 days was a sufficient period of time to perform analyses on the videos captured during the tests. However, the program team has now determined that a longer retention period is required to adequately conduct the research, perform analyses, and report results. The extended retention period will enable vendors to go back and test their algorithms on their old data sets as well as new ones provided under this program. Therefore, the data retention will be extended until the conclusion of the program, now scheduled for 2014.

The Data Protection Requirements address the risks associated with extended retention discussion, (e.g., unauthorized use or access to information)**.** NDAs, required prior to receiving any data, are the foundation of the data protection strategy by binding the signatory to the multiple data protection requirements.

Internal Sharing and Disclosure

There are no changes in internal sharing and disclosure of information.

As stated in the initial PIA DHS/S&T shares the high-level, summary results of the study with the Transportation Security Administration (TSA), Office of Bombing Prevention and the U.S. Secret Service. STIDP may share data within DHS S&T (e.g., Human Factors Division).

External Sharing and Disclosure

The sharing of data externally with DoD (a funding client), other government agencies (strategic partners), and relevant industry (technology providers) will help communicate a common set of technical and operational requirements, leverage the activities of STIDP with agencies performing similar research, and motivate industry to develop technology-specific solutions. Each will help accelerate the development of a deployable solution for DHS Components and DoD.

This PIA update reflects new external sharing of PII (crowd video images) captured at the Toyota Center and other public venues to entities that are not under contract to PNNL.

The privacy risks associated with the external sharing and disclosure may be unauthorized disclosure or inappropriate uses of the video data. These risks are mitigated by a multi-layered approach to information security as documented in the Data Protection Requirements discussion. NDAs, required prior to receiving any data, are the foundation of the data protection strategy by binding the signatory to the multiple data protection requirements.

Notice

As with the original PIA, PNNL will provide notification to the public at all venues while testing of modules collecting video images is in progress. As defined by the Live Event Testing Requirements, notification will take the form of signs posted strategically at key points in the venue. The signage will inform the public that 1) video surveillance or other sensor testing is occurring and 2) an alternative approach to the venue is available for individuals that wish to avoid the surveillance/screening activities.

Individual Access, Redress, and Correction

No additional changes have been made regarding the access, redress, and correction of information by individuals. Consistent to the original PIA, individuals may not gain access to their information. No additional PII will be collected to associate an individual in an image; nor will the public have access to the images.

Technical Access and Security

A privacy risk associated with the wider distribution of the video data sets is that data will be copied or used for unauthorized reasons or that unauthorized users will have greater access to the video. These risks are mitigated by a multi-layered approach to information security as documented in the Data Protection Requirements discussion. NDAs, required prior to receiving any data, are the foundation of the data protection strategy by binding the signatory to the multiple data protection requirements.

Technology

Changes to the technologies being considered is the addition of first-line sensors (i.e., magnetometers, electronic nose) and additional standoff technologies. The use of video camera for situational awareness and object tracking was documented in the original PIA.

The magnetometer works by measuring the perturbation of the local magnetic field. The sensors are targeting relatively large masses of metal— for example, inventories are far greater than most medical devices. The electronic nose technology works by detecting traces of chemicals in a specific area. These specific first-line sensor technologies pose no additional privacy risks, as they only detect the presence of

metal objects or explosive chemicals. Both are not capable of collecting any PII. Because video cameras will be used to record events in the vicinity of the first-line sensors, PII can be generated while testing with this system. To mitigate privacy risks, the Data Protection Requirements will be applied to PII data generated with live crowds.

The additional standoff technologies include: passive and active SMMW, THz imaging and sensor technologies and acoustic imaging and sensor technologies. These technologies operate similarly to the approved MMW technologies documented in the original PIA. PNNL will be evaluating the suitability of these systems for inclusion into the PBIED architecture under development. While these technologies alone are not capable of collecting PII or identifiable images, the sensor system will typically include a video camera. Thus, PII can be generated by this system. The Data Protection Requirements will be applied to data generated with live crowds; the Live Event Requirements (i.e., providing public notice and opt-out options) will guide live testing and the Law Enforcement Operations Requirements will be levied when law enforcement or security personnel serve as operators.

Appendix A: Table of Standoff Technologies

Technology Type	Technology Description	Technology Purpose	Technology Decision Process	Identifiable Image?
Passive[3] Millimeter Wave (MMW), Submillimeter Wave (SMMW) and Terahertz (THz) Imaging	Uses natural MMW, SMMW or THz illumination emitted and reflected from a person and the surrounding environment. A video camera is integrated into this system.	Detects the presence of concealed objects on a person's body.	Not automated: Properly trained operators scan crowd looking for image anomalies indicative of concealed weapons. (It is not possible to identify a person from these images.) Automated: System detects image anomalies which alerts an operator for confirmation, or used directly as indication of concealed weapons	MMW, SMMW, THz image: No Video image: Yes

[3] Passive imaging technology uses only what is available to create the image (e.g., non-flash photography).

Technology Type	Technology Description	Technology Purpose	Technology Decision Process	Identifiable Image?
Active[4] Millimeter Wave (MMW), Submillimeter Wave (SMMW) and Terahertz (THz) Imaging	Uses MMW, SMMW or THz illumination reflected from a person and the surrounding environment. A video camera is integrated into this system.	Detects the presence of concealed objects on a person's body.	Not automated: Properly trained operators scan crowd looking for image anomalies indicative of concealed weapons. (It is not possible to identify a person from these images.) Automated: System detects image anomalies which alerts an operator for confirmation, or used directly as indication of concealed weapons	MMW, SMMW, THz image: No Video image: Yes
Passive and Active MMW, SMMW and THz Sensors	While an image is not generated, a signal from the device can detect the presence of an anomaly on a person's MMW, SMMW or THz signature. A video camera is integrated into this system.	Detects the presence of concealed objects on a person's body.	Can be automated or operated manually. Output is a graphic (typically a chart) showing signals over the course of time the person is in the device's range. A threshold can be set such that an alert is triggered if the signal reaches an abnormal level for the environment.	MMW, SMMW or THz sensor output: No Video image: Yes

[4] Active means the imaging technology illuminates the subject to create the image (e.g., flash photography).

Technology Type	Technology Description	Technology Purpose	Technology Decision Process	Identifiable Image?
Infra red (IR) Thermography (passive)	Uses the IR energy naturally emitted and reflected by the human body. IR frequencies in the LWIR, MWIR or SWIR may be used. A video camera is integrated into this system.	Concealed objects are observed with IR imaging systems.	Not automated. Properly trained operators scan crowd looking for IR image anomalies indicative of concealed weapons. Relies on operator judgment to make detections. (It is not possible to identify a person from an IR thermography image.)	IR image: No Video image: Yes
Video surveillance cameras	Commercial-off-the-shelf still camera[5] and video surveillance systems capable of recording live images (no audio will be included).	Used as an expanded view of the screening zone where other technologies are more likely to be focused on a smaller area.	Will be operated manually and use data to compare to other technology outputs for accuracy research.	Yes
Intelligent Video Systems	Multiple fixed video cameras coupled with image processing software (i.e., video analytics). The video analytics software compares images over time and identifies anomalies based on user-defined rules.	Used to detect, locate, and track leave-behind objects and individuals to identify anomalous behavior.	Can be automated or operated manually. Software will process all images and uses algorithms to detect anomalies.	Yes

[5] Still camera is a camera that takes a single picture, a digital camera with video capabilities.

Appendix B: Table of New Standoff Technologies

Technology Type	Technology Description	Technology Purpose	Technology Decision Process	Identifiable Image?
Video surveillance cameras	Commercial-off-the-shelf still and video surveillance systems capable of recording live images (no audio will be included).	Used as an expanded view of the screening zone where other technologies are more likely to be focused on a smaller area.	Will be operated manually and use data to compare to other technology outputs for accuracy research.	Yes
Magnetometers and Metal Detectors	Passive magnetometers (detect ferrous metal) or active metal detectors (detect all metals).	Used to detect metal carried by a person. May be indicative of a concealed weapon.	Automated: System generates alarm if an anomaly is detected. Video cameras are used to identify the person or persons causing the alarm.	Magnetometer /metal detector alarm: No Video image: Yes
Electronic Nose	Chemical sensors which sample the air and identify vapors which may be indicative of the presence of explosives nearby	Used to detect the presence of explosives	Automated: System generates alarm if an anomaly is detected. Video cameras are used to identify the person or persons causing the alarm.	Chemical sensor alarm: No Video image: Yes

Technology Type	Technology Description	Technology Purpose	Technology Decision Process	Identifiable Image?
Acoustic Imaging and sensors	Uses ultrasound waves reflected from the body.	Detects the presence of concealed objects on a person's body.	Not automated: Properly trained operators scan crowd looking for image anomalies indicative of concealed weapons. (It is not possible to identify a person from these images.) Automated: System detects image anomalies which alerted an operator for confirmation, or used directly as indication of concealed weapons	Acoustic image: No Video image: Yes

Responsible Official

Joe Foster, Program Manager

Science and Technology Directorate

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security