Privacy Impact Assessment
for the

Standoff Explosives Detection Technology Demonstration Program

August 28, 2008

Contact Point
Joe Foster
Explosives Division
Science & Technology Directorate
202-254-5314

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

Abstract

The DHS Science and Technology Directorate (S&T) initiated the Standoff Explosives Detection Technology Demonstration Program (SOTDP) in March 2007. This is a multi-year research and development program (through 2013) designed to accelerate the development of explosive countermeasures—standoff technologies, concept of operations (conops), and training to prevent explosive attacks at large public events such as conventions, concerts, sporting events, public celebrations, etc. The purpose of this program is to develop an integrated system of devices to improve security and public safety, while not impacting pedestrian traffic flow or violating personal freedoms and individual privacy. DHS S&T is sponsoring the SOTDP and associated demonstrations in a multi-year R&D initiative. S&T has a program management and oversight role in the project, which includes providing policy direction and input on program requirements. This PIA is being conducted because personally identifiable information will be collected during the R&D process.

Overview

The SOTDP's predecessor program, the Rail Security Pilot was also focused on the development of the explosive countermeasures and was divided into two phases. Phase I, conducted in February 2006, did not require the collection of personally identifiable information (PII) and evaluated existing countermeasures using aviation security methods that could be implemented immediately. Phase I technologies included walk-through metal detectors and dual-energy X-ray machines that were modified for the rail threat basis (i.e., large amounts of metal typical of that found in suicide bomber vests and large quantities of explosives capable of damaging key infrastructure).

Phase II evaluated emerging technologies with varying technological maturity. Phase II activities occurred in several locations and the accompanying Privacy Impact Assessment (PIA) addressed the collective Phase II demonstration effort. The Rail Security Pilot evaluated over 14 different explosive detection technologies, and developed unique operating protocols and training curricula to minimize the burden of responding to an explosive attack on the rail sector. The RSP provided valuable insights as to the challenges of screening a mass transit subway station. To truly accelerate the development of a viable countermeasure architecture, S&T determined that a longer-term test and evaluation program focused on technology development, systems integration, conops improvements, and standards was needed.

As a result of the Rail Security Pilot, the SOTDP was established to initiate a multi-year field testing program to accelerate the development of promising standoff detection architectures.

The SOTDP uses National Planning Scenario 12 (NPS-12) as its threat planning basis. NPS-12 describes a multi-pronged, coordinated attack involving suicide bombers, vehicle-borne improvised explosive devices, and leave-behind bombs. Thus, the SOTDP is charged with developing the security architecture that could be deployed in response to a multi-threat NPS-12-like event. This security architecture will include standoff explosive detection technologies.

There are two general classes of standoff technologies: technologies that detect anomalies (such as a concealed object or large amounts of metal), and technologies that detect the chemical signature of explosives or their constituents. The near-term focus is on anomaly detection.

Prior to testing in the field, research organizations will conduct independent laboratory and/or field testing of the equipment to evaluate sensor performance and readiness for deployment at a public event such as a hockey game. In fact, other government agencies have already conducted similar tests including: Technical Support Working Group, Joint Improvised Explosive Device Defeat Organization, Night Vision Laboratory. This layered approach to testing ensures that before the technology is tested publicly, all prerequisite issues have been addressed and the only outstanding issues are those which can only be addressed through public testing.

Upon successful laboratory testing, S&T plans to conduct field demonstrations of promising standoff technologies over the course of the program. If necessary, limited-scale outdoor "readiness testing" will be conducted at the Pacific Northwest National Laboratory (PNNL) in Richland, Washington prior to field testing to obtain initial indications of sensor and system performance in an operationally relevant environment. In a number of cases, the sensors have been tested outdoors under prototypic conditions, thereby eliminating the need for this type of testing.

Once a technology has been determined to be ready for field testing, demonstration of the actual proposed countermeasure (e.g., combinations of technologies) will be conducted at actual public events because factors such as crowd diversity (e.g., body type), crowd behavior, quantity of subjects, and integration with an existing business process cannot adequately be captured in a lab/campus environment.

PNNL has approached and has negotiated an agreement with a local 6,000-seat venue (the Toyota Center located in Kennewick, Washington) to serve as a long-term testbed for the project. It is expected that demonstrations of standoff technologies would be conducted approximately twice per year. Additional field demonstrations may also be conducted at other venues to address differences in venue size, people flow, and operations. The combination of PNNL and the Toyota Center provides DHS with exceptional testing flexibility.

The SODTP team includes the Department of Homeland Security's Explosives Division (Science and Technology Directorate), Pacific Northwest National Laboratory, MITRE, and subsequent technology vendors. DHS S&T will not operate the equipment being tested (the equipment will be operated by the Kennewick Police Department (KPD) with supervision from SOTDP researchers), but will observe the demonstrations and will have access to and own all the data collected. Pacific Northwest National Laboratory (PNNL) will serve as the technical prime contractor for the SOTDP. PNNL's role includes architecture development, facility logistics, technology maturation and acquisition, deployment of overall systems, operator training, testing, data evaluation, and reporting. PNNL and/or their equipment vendors will be onsite for all demonstrations to train operators, provide assistance during operations, and troubleshoot equipment. PNNL will store data for DHS S&T, but will not own the data. MITRE will provide system integration and analysis. Throughout this document, the term "SOTDP research team" refers to DHS S&T program management and PNNL and MITRE technical experts. Vendors will provide screening technologies for testing in the SOTDP. Vendors will contribute to the architecture design and provide training and technical assistance. Vendors will temporarily have access to raw data collected during demonstrations, but only that information that relates to the vendor's technology.

The SOTDP is charged with making progress in the following areas over the course of its seven-year life: increased technical functionality, increased systems integration, improved ConOps/interdiction approaches, technical and operational standards development, and industry motivation. Increased technical functionality translates into more people screened, more quickly, with improved technical performance.

Increased system integration addresses the need for single and multi-modal data fusion and an integrated command and control structure that can address multiple, simultaneous threats (e.g., suicide bombers and vehicle-borne improvised explosive devices). Improved ConOps/interdiction processes attempt to automate all or part of the interdiction/secondary screening process such that maximum protection is afforded to security personnel. Standards will be developed for standoff threat articles and standoff test protocols; industry standards for the integration of discrete detection systems will also be addressed. Finally, strategies to motivate industry to invest in standoff systems and their integration will be rolled out over the length of the program such that more and better equipment will be available to test.

S&T plans to test a selection of imaging and sensing technologies. A video camera will record images of the same field of view as the sensors resulting in both video images and raw sensor data of the people within the testing area. The raw sensor images do not show enough visual details to identify a person; however, the accompanying video camera image can be used for identification.

The video images captured during testing at the public venue may be used in the following ways.

1) By law enforcement to ensure that if a sensor identifies a suspicious object, law enforcement personnel can accurately associate the sensor alert with the physical appearance of the individual associated with that alert.

2) To potentially improve sensor performance; however, it is unlikely that the video image alone could be used to improve sensor performance (it would need to be correlated with the actual sensor image to be of value).

3) To communicate to the security community the nature of tests conducted. The SOTDP research team will blur the face of any video camera image released outside of the project team (e.g., for use in technical reports or conferences) to protect the individual's privacy.

4) To record the nature of the crowd flow from various points on the property. Understanding crowd flow is very important with respect to optimizing the placement of equipment. By recording crowd flow as a function of time, we can propose alternative locations for our sensors to optimize the number of people screened as well as methods to increase the flow of people down predefined screening lanes. The information captured by the surveillance cameras (number of people arriving as a function of time) will also be used to compute the percentage of arriving patrons screened (based on the number of screens in the same period).

Technology Type	Technology Description	Technology Purpose	Technology Decision Process	Identifiable Image (Yes/No)
Passive[1] Millimeter Wave (MMW) Imaging	Uses natural MMW illumination emitted and reflected from a person and the surrounding environment. A standard 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 a MMW image.)	MMW image: No[2] Video image: Yes
Passive terahertz imaging	Very similar to millimeter wave imaging with a slight shift in measured electromagnetic energy naturally emitted from the human body. A standard 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 a passive terahertz image.)	Terahertz image: No[2] Video Image: Yes
Passive and Active MMW Sensors	While an image is not generated, a signal from the device can detect the presence of an anomaly on a person's millimeter-wave signature. A standard 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 sensor image: No Video image: Yes

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

[2] Technology image output is not identifiable; however, the device has a standard on-board camera that will provide a still image along side the unidentifiable image to identify which person to perform further screening on.

Technology Type	Technology Description	Technology Purpose	Technology Decision Process	Identifiable Image (Yes/No)
Infra red Thermography (passive)	Uses the IR energy naturally emitted and reflected by the human body. A standard 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[2] Video image: 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
Standard 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

Two different types of testing may be conducted at PNNL prior to testing at the public venue: readiness testing of technologies to determine whether they are mature enough to operationally deploy at a public event and integration testing to characterize the various technologies as an integrated countermeasure "system." The SOTDP team will conduct readiness testing in an isolated area on the PNNL campus. For readiness tests, PNNL staff will operate the equipment and will screen only volunteer members of the PNNL SOTDP team. Integration testing will be conducted along a pathway leading to two high-occupancy buildings on the PNNL campus and will screen individuals approaching the buildings. Individuals seeking access to these buildings need a Department of Energy Badge for entry; visitors can be badged at several locations on campus. The vast majority of individuals approaching these buildings are PNNL staff; however, Department of Energy staff visitors, and the general public can also access the buildings (one of the buildings has several conference rooms near the entrance that can be accessed by the general public). Signage will be posted, similar to that described below, notifying the public and staff that screening would be taking place and that persons not wanting to participate could enter the building from another entrance. Testing would also be announced through lab-wide electronic communications tools that are routinely used to communicate weekly events and items of interest to staff.

In the event of an alert by a sensor, an SOTDP team member will inform the individual that the team is conducting experimental testing of screening technologies and ask the individual if they would be willing to answer a brief set of questions concerning what they were carrying on their person. Individuals would not be required to answer questions if they so desired. Law enforcement would not be involved in the testing at all unless a clear threat was identified. In such a situation, the staff member would call the PNNL emergency desk who would alert the Hanford Patrol and/or the Richland Police Department. (Note that the entire PNNL campus is covered by a series of surveillance cameras. These cameras could be used to track threats into parking lots.) The SOTDP team has briefed PNNL on the proposed experiment as described above, and PNNL has approved readiness and integration testing by the SOTDP.

Once successful readiness testing at PNNL concludes and the SOTDP research team determines that the technology operates accurately and reliably, the research team will initiative the public venue phase of testing.

The public venue will be the Toyota Center--a multi-purpose venue that is home to professional hockey and football teams. In addition to the professional sporting events, the venue holds concerts, Broadway-type shows, local high school and college graduations, regional indoor sporting events, and religious gatherings. The heaviest user of the Toyota Center is the Tri-City Americans hockey team. The Toyota Center is operated by VenuWorks on behalf of the Kennewick Public Facilities District (KPFD). Security for events is provided by VenuWorks and the Kennewick Police Department (KPD). The KPFD, KPD, Tri-City Americans, and VenuWorks have all approved field testing by SOTDP.

In conducting the tests at PNNL, the Toyota Center, or any other venue, the SOTDP team will adhere to a set of operating principles in order to achieve compliance with federal privacy laws and DHS privacy policies, as well as federal regulations governing human subjects testing. (PNNL's human subjects testing protocol and approval will be reviewed by a registered Institutional Review Board as appropriate and by the DHS Regulatory Compliance Office to assess compliance with DHS requirements.)

SOTDP's operating principles for conducting field tests at PNNL, the Toyota Center, and/or any other venue include the following:

- Because the focus of the research is to test screening technologies at a distance, the actual use of the SOTDP technologies will occur on pathways leading to the event or building, before the entrance gate of the event or building. On that pathway, well before the entrance and outside the range of the SOTDP screening technologies, individuals will be given the opportunity to choose whether or not to participate in the research effort. Individuals choosing to participate will proceed in a direction down a pathway screened by the SOTDP technology. Individuals choosing not to participate will proceed in a different direction down a different pathway to arrive at the event/building and stay outside the SOTDP technology's field of view.

- Signage will be posted at strategic locations indicating that persons using the SOTDP approach will be subject to DHS security screening and surveillance cameras. The signage addresses two important elements of testing: consent for searches and consent for capturing personally identifiable information (via video). (Note that the PNNL campus operates facility surveillance cameras.)

- The SOTDP team will ensure compliance with all federal regulations governing human subjects testing and obtain approval from the DHS Regulatory Compliance Office prior to testing.

- To the extent possible, the SOTDP research team will use local law enforcement as operators of the equipment (e.g., KPD, Richland Police Department, Hanford Patrol, Benton County Sheriff's Department, etc.). This will enable the SOTDP research team to receive feedback from the actual future operators (e.g., law enforcement) as to the usability of the equipment. The SOTDP research team will train the law enforcement officers on how to operate the SOTDP equipment and the significance of images law enforcement officers would see through the SOTDP equipment. Even in situations where law enforcement personnel are not operating equipment, law enforcement personnel would still be responsible for making any operational or law enforcement decisions based on threat objects identified by the experimental technologies.

- For testing at any public venue (e.g., non PNNL testing), all contact with the public due to an alert by the sensors will be handled by local law enforcement. The sensor's video image will be used by the KPD[3] to ensure that, should they approach an individual based on a sensor alert, they approach the same individual the sensor identified. KPD officers will address the threat per their standard operating procedures. As with all other points of entry at the event, law enforcement personnel will make all determinations as to whether a suspected threat requires resolution and how to proceed with such resolution. Based on the SOTDP research team's explanation of the images from the SOTDP equipment, if KPD personnel determine that resolution is required, they will implement a graded interdiction approach. For the lowest perceived threats (e.g., a suspicious object in a person's pocket), the KPD may ask the individual a few simple questions. For threats of greater concern (e.g., unidentifiable concealed objects or identifiable objects such as weapons), a physical search may be conducted by the KPD based on existing law enforcement protocols and requirements. Irrespective of the interdiction approach, if nothing is found then the individual will continue on their way with no collection of additional personal information.

[3] KPD has jurisdiction over the Toyota Center, but will allow other local law enforcement agencies to participate as operators of the equipment, thereby increasing the region's awareness of new technologies and reducing their manpower investment. While other law enforcement agencies or other entities may operate the equipment, KPD will call for and perform interdictions of persons of interest.

- All data collected by the SOTDP team will be tightly held as described in Sections 2.4 and 3.4. All video images will have facial features blurred if the images are shared outside the SOTDP research team as discussed previously.
- If formally requested for criminal proceedings, DHS may provide the KPD a copy of the image or photo that prompted the primary screening process, as appropriate under state and federal laws and DHS legal and privacy policies. Any such request by the KPD would be referred to the DHS General Counsel and the DHS Privacy Officer for appropriate action.
- The images collected during field testing will subsequently be analyzed to support the program's research objectives and drive future technology enhancements. This analysis will seek to determine whether each technology accurately identified anomalies and what factors contributed to the success/failure rate for each technology.

S&T is planning regular demonstrations at PNNL and the Toyota Center. This PIA will be updated to reflect additional technologies and sites as future demonstrations are planned. It is envisioned that as the SOTDP program matures, field demonstrations at more challenging venues may be conducted.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed. Jurisdiction

1.1 What information is collected, used, disseminated, or maintained in the system?

Sensor data and/or images and integrated video images of individual patrons traversing the detection area will be collected using the technologies described in the Introduction to assess the potential presence of concealed threats such as improvised explosive devices or other weapons. Operators (the KPD) will be trained by the program's technical team to distinguish between normally concealed objects (e.g., cell phones) and concealed objects that may pose a threat. The images collected will only contain date/time or sequence number labels – aside from the images of individuals, no other identifying information about those individuals will be collected.

DHS S&T and its contracted research team will create alarm resolution reports that document what objects, if any, were found and where (e.g., PDA and cell phone in left trouser pocket). Based on the information provided by the SOTDP research team about the object detected by the sensor, the KDP will use its professional judgment to determine whether to approach the individual. If the visual information provided to the operators by the sensor(s) indicate the presence of a cell phone or equivalent sized object, the individual will be allowed to proceed to the gate. If the visual information provided by the sensor(s) indicate the presence of a prohibited item (e.g., weapon) or a possible explosive threat and KPD determines that it is appropriate to approach the individual, the KPD will collect additional information from the individual through visual inspection, direct questioning, or (should the KPD deem it necessary) a pat-down. The SOTDP research team will not collect any additional personal information other than the video and sensor data described in this PIA (i.e., the SOTDP team will not collect individuals' names). The KPD

may collect additional information per their standard operating procedures. If formally requested for criminal proceedings, DHS may provide the KPD a copy of the image or photo that prompted the primary screening process, as appropriate under state and federal laws and DHS legal and privacy policies. Any such request by the KPD would be referred to the DHS General Counsel and the DHS Privacy Officer.

1.2 What are the sources of the information in the system?

At the clearly marked SOTDP approach to the Toyota Center, the KPD will operate the SOTDP screening technologies and those SOTDP screening devices will record copies of the screening images that will be used by the SOTDP research team to assess the SOTDP technologies. All event attendees who pass through the SOTDP approach will be screened for concealed body-borne explosive threats as they progress through the SOTDP screening technology. The technologies described in the Introduction will collect sensor output or images directly from individuals to identify a threat. Depending on the technology, an alert may be triggered based on a subjective interpretation of the sensor output by an operator, or by an automated algorithm. Automated anomaly detection can be manually overridden if the operator suspects a threat or makes the determination that no threat is present.

Equipment operators will be KPD personnel who have been trained by the SOTDP research team and/or their vendors to interpret data and make further determinations regarding suspect threats. Standard video surveillance cameras are included in the SOTDP technologies so that a person of interest can be subsequently identified in a crowd, stopped, and questioned. All video data will be carefully controlled by the SOTDP research team per the requirements outlined in this PIA. The images from the surveillance cameras will only be used in support of the SOTDP research project and for no other purpose. DHS S&T may provide supporting data (e.g., photo for criminal proceedings in accordance with state and federal law and DHS legal/privacy policies) upon formal request by the KPD authority, and review by the DHS Office of General Counsel and the DHS Chief Privacy Officer.

Toyota Center security will use traditional screening technologies (hand-held metal detectors and/or physical bag searches) at the gate areas to screen all individuals entering the event.

1.3 Why is the information being collected, used, disseminated, or maintained?

The purpose of the SOTDP is to assess the merits of available, emerging technologies to mitigate the threat of a body-borne explosive device or leave-behind bomb at large public events. The information collected by the devices provides an indication of a potential threat that may require secondary assessment by KPD officers. KPD officers will make this determination and will manage any detected threats per their standard operating procedures. These technologies and security systems must be evaluated at a highly attended venue event to ensure operationally relevant data is collected.

1.4 How is the information collected?

The information is collected using the technologies described in the Introduction. In general, each device has the ability to collect and store sensor data. A data acquisition system will be used to capture data from each device's operating computer or display. The data acquisition system will also collect relevant environmental data to evaluate external factors that could have affected sensor system performance.

1.5 How will the information be checked for accuracy?

The accuracy of the information is determined by the detection that takes place. The program is seeking to detect concealed threats, such as a bomb. All positive indications of a threat from the surveillance technologies will trigger the KPD officer's interdiction process. The individual may be subject to a pat down if onsite KPD determines that further screening is necessary. Potential threats will be resolved as nuisance (the item causing the alert was appropriately found, but was not a threat), false (no item was found), and true (the item found was a true threat).

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support R&D related to improving the security of the homeland. The KPD will operate according to its existing legal authorities and standard operating procedures.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

This multi-year program is designed to evaluate the merits of commercial and near-commercial technologies (i.e., technologies that are largely developed but are not yet commercially available) to identify suicide bombers among venue patrons in real-world exercises. Several of the technologies capture traditional visible photographic/video images with emerging "invisible to the eye" images of body-borne concealed threats or raw signal strength and data. The images are being collected to enable S&T to evaluate the performance of these technologies in accurately identifying threats and are used by the KPD to interdict a person of interest.

There is a privacy risk associated with the whole body photographs or videos that accompany the direct sensor output. As discussed in the table in Section 1.1, it is not possible to identify a person based on IR, MMW, or THz images. The privacy risk has been greatly reduced by not collecting any additional personally identifiable information (such as name); thus individuals remain anonymous to DHS and the SOTDP research team. In addition, individuals can choose to opt out of the SOTDP screening process. The approach to the event where the SOTDP technologies are deployed will indicate the use of research technology to improve the screening process.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Information is collected in the form of patron images as follows:

- Traditional surveillance camera video will be deployed in the SOTDP test area to record crowd dynamics such as the arrival rate and behavior of patrons as they progress through the detection zone. These same cameras will be used to ensure that a person of interest has been successfully interdicted. The camera images will be processed using video analytics, algorithms to identify anomalies. Note that existing KPD surveillance cameras will already be deployed as part of event security procedures; however, these images will not be integrated into the SOTDP data acquisition system nor will SOTDP have access to those images.

- The infrared (IR), terahertz (THz) and millimeter wave (MMW) scans of patrons will be used to evaluate explosives detection technology effectiveness derived from pooled data.

All of the images collected are part of a research experiment designed to test the ability of these technologies to identify concealed explosives or other threat objects carried on the patron's person. Information collected for this program will be held within the program to derive statistical measures of performance for each system. If the system identifies a possible concealed explosive threat, an alert will occur. Resolution is required on all primary detection alerts. All alerts will be referred to the KPD for further (i.e., secondary) screening. The onsite SODTP research team and/or their vendors will assist the KPD officers interpret alerts from the SOTDP equipment. The KPD authorities will manage the secondary inspection/alert resolution process according to the same standard operating procedures used at the other points of entry at the event. If the KPD determines that a pat-down is required, then alarm resolution will require actual verification. If the KPD determines that a pat-down is not required, then actual verification may not be required. KPD will make these decisions.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The information will be analyzed to estimate measures of effectiveness, such as probability of detection, false positive rate, nuisance alert rate, and impact on the individual. To the extent possible, alarm resolution reports will be correlated with an image or sensor signal such that the vendors can better understand the source of the alarm and further develop the technologies. Each vendor will have data analysis methods specific to their technologies.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

No commercially or publicly available data will be used.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Only the SOTDP research team will have access to the data collected except in the event of a formal request by the KPD for criminal proceedings. In the event of a formal KPD request, DHS may provide the KPD a copy of the image or photo that prompted the primary screening process if DHS has not yet destroyed the images per the retention practices discussed in Section 3 and if providing the image is deemed by DHS General Counsel to be appropriate under state and federal laws and DHS legal and privacy policies. Any such request by the KPD would be referred to the DHS General Counsel and the DHS Privacy Officer.

Technology will be deployed to blur the images of faces or other identifying features when images are shared outside of the SOTDP research team. All SOTDP research team members using the data collection system will be trained on the appropriate use of the system and the collection of the information so as to decrease the risk of misuse of the images.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The images produced by the SOTDP equipment will be retained in order to assess the performance of the technology and to plan further research efforts.

3.2 How long is information retained?

The data will be analyzed by the DHS SOTDP research team for a period not to exceed ninety (90) days, after which the data will be destroyed. Ninety (90) days provides adequate time to complete the SOTDP data analysis and develop follow-on actions.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. General Records System 20 covers the disposition of Electronic files or records created solely to test system performance, as well as hard-copy printouts and related documentation for the 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."

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The information needs to be retained for 90 days to ensure adequate time is available to assess the utility of the technologies being evaluated and to update the training materials, if necessary. During the period the data is retained, the data will be password protected, as well as access restricted. The data will protected by a network firewall when uploaded to electronic file storage areas. The risks of retention will be mitigated by destroying the data after 90 days.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

DHS/S&T will share the high-level, summary results of the study with the Transportation Security Administration (TSA), Office of Bombing Prevention and the U.S. Secret Service. The individual images will not be released unless facial features are obscured/blurred to prevent identification of the individual. The purpose of sharing the information is to assess the merits of technology systems/concepts of operations for other DHS Components.

4.2 How is the information transmitted or disclosed?

The study results and associated obscured/blurred pictures will be transmitted in electronic or print form. All reports generated by the program will be marked with the appropriate classification marking and will be maintained according to the requirements of that designation. File transmission will be encrypted and/or password protected.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Internal information sharing is needed within the SOTDP research team to understand and define the technology and conops merits/demerits. Sharing outside the SOTDP research team is necessary to provide summary results to key stakeholders. All images shared *external* to the SOTDP research team will have blurred facial features to prevent identification of the individual. The risk associated with internal sharing would be the unauthorized disclosure of an individual's image. To mitigate this risk, only the SOTDP research team will have access to the clear 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 DHS which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Technology system performance results will be shared to enable government agencies to evaluate operational performance, costs and benefits of technologies employed in the test. No personally identifiable information will be shared. Study results will be available to government agencies and Congress in the form of a briefing and formal report. Commercial vendors supplying equipment for the program will have temporary access to the images during the demonstration. These vendors will be provided generalized results of their technology's performance and the performance of the overall field demonstration in order to facilitate maturation of the technology.

Should secondary screening confirm the presence of concealed weapons or illegal drugs, the KPD will respond as appropriate. DHS S&T may provide supporting data (e.g., photo for criminal proceedings in accordance with state and federal law and DHS legal/privacy policies) upon formal request by the KPD authority, and review by the DHS Office of General Counsel and the DHS Chief Privacy Officer. S&T can locate specific images by searching for time cues or alarm number.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing is compatible with the purpose of the original collection. Because the data will not be retrievable by personal identifier and the images will be blurred when shared outside the SOTDP research team, a SORN is not required.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Printed or electronic summary reports of the study will be provided without any personally identifiable information. Electronic transmissions will be password-protected and/or encrypted. Sensitive security information resulting from the SOTDP will be protected according to DHS information security requirements.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

For results presenting a camera image of an individual, the facial features will be obscured or blurred prior to sharing so that no personal information is provided to anyone external to the SOTDP research team. For KPD authorities, the clear image photo may be provided (in accordance with state and federal laws and DHS legal/privacy policies) if formally requested for criminal proceedings.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

The approach to the venue where the SOTDP technologies are set up will be clearly marked, indicating that experimental screening technology will be used along with nature of that technology. Individuals will be given the choice to participate in the research effort or to use of the other points of entry. The KPD screening standards will apply at all points of entry meaning everyone attending the event will be subject to the same level of security screening. The signage that will be used has not yet been developed, but will be very similar to that used for the Rail Security Pilot. S&T will work with the Civil Rights and Civil Liberties Office to develop appropriate notice. Below is an example of similar signage used in the Rail Security Pilot:

> "Passenger Advisory, Exchange Place Station, February 6 – March 1, 2006
>
> The U.S. Department of Homeland Security, in cooperation with PATH, a subsidiary of the Port Authority of New York and New Jersey, is conducting a pilot project to test the effectiveness of explosives detection systems to protect rail rapid-transit passengers.
>
> Notice: All passengers entering the PATH Exchange Place Station are advised that they and their carry-on items, may be subject to a security inspection, upon request.
>
> Passengers who do not agree with such inspection will not be allowed to enter the PATH system at Exchange Place and must exit this station."
>
> Alternative means of entering the venue will also be afforded to the patrons.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

The notice, as described in 6.1, will provide prominent notice to patrons of their options including the opportunity to enter the venue where the test will take place or choose to enter via another gate thereby opting out of the program study with no record of declination or penalty.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. Once the patron chooses to enter the inspection area as defined by temporary signage, the person has consented to have images obtained by the SOTDP research team.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Individuals will be provided adequate notice, as described in 6.1, that security screening will occur en route to the chosen venue gate. An individual may choose not to have their images collected by entering the venue through a separate gate. Sufficient notice of the location and type of screening has mitigated the risk of the individual being unaware of the collection of information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals may not gain access to their information. No additional personally identifiable information is collected to associate an individual in an image, nor will the public have access to the image database. Nonetheless, if a person is arrested based on illegal activity identified by the images and by KPD secondary screening, they may request copies of these images from the KPD.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If alarm resolution is required, a graded interdiction approach will be implemented by KPD authorities, according to KPD standard operating procedures. For the lowest perceived threats, the KPD may conduct a brief interview with the individual. For threats of greater concern, a physical search may be conducted by the KPD. Irrespective of the interdiction approach, if nothing is found then the individual will be allowed to continue on their way and no personal information will be collected. The individual will be identified for secondary screening by comparing the image associated with the sensor alert (see above discussion) to the individual being screened. In all scenarios, the KPD will follow its standard operating procedure for security screening and will be fully supported by the onsite SOTDP research team.

7.3 How are individuals notified of the procedures for correcting their information?

As noted in 7.2, any necessary corrections will occur during the screening process. Therefore, there is no information to be corrected.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The individual has the alternative of not participating in the study by entering the venue through a separate approach.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Individuals will not have access to collected images. No personally identifiable information besides the images is collected, thus the images are not catalogued by retrievable personal information. The risk to the individual would be a false positive erroneously indicating that he or she was transporting explosives or related materials. Any such erroneous information will be corrected during secondary screening by the KPD.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Only the SOTDP research team will have access to both the clear and blurred images collected while in the field, and later during data analysis/summary report preparation. Team members must request access from the SOTDP Technical Director. Access will be granted on a need-to-know basis.

KPD surveillance cameras would be capturing clear images of individuals regardless of the presence of SOTDP technologies. The SOTDP surveillance cameras discussed in the table in Section 1.1 do not create blurred images. The SOTDP research team has committed to blur any images collected if they will be viewed by anyone outside the SOTDP research team. The images will be retained as part of the research project. An image will be correlated with an assessment (provided by local LE) of what the person may have been carrying at the time to cause an alert. This will support further R&D to refine the technologies and reduce the false positive rate.

8.2 Will Department contractors have access to the system?

Yes. PNNL, a U.S. Government National Laboratory, and MITRE will have access to the system. Commercial vendors supplying technology for the program (operating under contract with DHS) will support the field operations, providing technical advice on optimum operation of the technologies. These vendors will have access to the data during the demonstration.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Appropriate privacy training will be developed and provided to the limited number of individuals on the SOTDP research team with actual access to the system.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The S&T CIO has confirmed that C&A is not required.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

To prevent the misuse of data, access to identifying images will be limited to the SOTDP research team. All contractors and vendors with access to any identifying data will sign non-disclosure agreements. Images shared with anyone external to the SOTDP research team will be blurred. All data will be protected by passwords and access to the data will be carefully controlled.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The privacy risk would be the unauthorized distribution of an individual's image. To mitigate this risk, access to the clear images is limited to the S&T research team. The bulk of image data collected will be translated into statistical performance characteristics of the technology by the DHS technical team. All S&T research team members have been trained on the appropriate use of the clear image. In addition, the images will be password protected, encrypted for transmission, and stored behind a network firewall.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The SOTDP is an R&D initiative designed to test the "real-world" performance of standoff explosives detection technologies in detecting explosive devices and related materials that could be used by a suicide bomber in a highly attended event venue setting.

9.2 What stage of development is the system in and what project development lifecycle was used?

Standoff explosives detection technologies are at various stages of development. Generally, the systems fall into technology readiness levels six to seven.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The program employs standoff detection technologies which capture video and/or still images of people being screened that could raise privacy concerns (again, a person can not be identified by the image collected in the IR, millimeter wave, and terahertz frequencies). To mitigate these concerns, facial images will be blurred when the images are shared outside the SOTDP research team, and no additional personally identifiable information will be collected or linked to the image.

The program has incorporated privacy concerns into the planning process. If deployed, full body imaging technologies will be configured so as to not show a revealing image of the screened individual. The SOTDP research team has also committed to blur any images collected if they will be viewed by anyone outside the SOTDP research team.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security