Privacy Impact Assessment
for the

Future Attribute Screening Technology (FAST) Project

December 15, 2008

Contact Point
Mr. Robert P. Burns
Science and Technology Directorate
Department of Homeland Security
(202) 254-6104

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

Abstract

DHS has identified a need for new technical capabilities that can rapidly identify suspicious behavior indicators to provide real-time decision support to security and law enforcement personnel. The Future Attribute Screening Technology Mobile Module (FAST) project, sponsored by the Science & Technology Directorate's (S&T) Homeland Security Advanced Research Projects Agency (HSARPA) and executed under the oversight of DHS S&T's Human Factors Behavior Sciences Division, seeks to develop people screening technologies that will enable security officials to test the effectiveness of current screening methods at evaluating suspicious behaviors and judging the implications of those behaviors. The ultimate goal of the FAST project is to equip security officials with the tools to assess potential threats rapidly. This first phase of the FAST project is limited to identifying various screening sensors and conducting testing of various sensors with volunteer participants.

Introduction

The DHS Directorate of Science and Technology (S&T) conducts homeland security research and leverages the scientific, engineering, and technological resources of the United States into technological tools to help protect the homeland. The Director of Innovation's mission is to support basic, applied, and advanced homeland security research to advance technologies that will promote homeland security. FAST is one such technology. FAST seeks to improve the screening process at transportation and other critical checkpoints by developing behavior-based screening techniques that will provide additional indicators to screeners to enable them to make more informed decisions. FAST is not intended to provide "probable cause" for law enforcement processes, nor would the FAST technology, once deployed operationally, replace or preempt the decisions of human screeners.

The baseline for the project is the development and validation of the Theory of Malintent. Malintent is the intent to cause harm. Although individuals may experience malintent in a variety of situations, the specific focus of FAST is identifying individuals who exhibit physiological indications, which in the specific screening settings, are determined to be associated with malintent. Behavioral scientists hypothesize that someone with malintent may act strangely, show mannerisms out of the norm, or experience extreme physiological reactions based on the extent, time, and consequences of the event. The FAST technology design capitalizes on these indicators to identify individuals exhibiting characteristics associated with malintent.

The scope of malintent has three distinguishing factors: the extent of planned harm, the future time horizon of the event, and the consequences to the individual who is planning the event. The extent of harm can range from individuals planning to cause a disturbance or use false documents to individuals who are planning an assassination or terrorist attack. The future time horizon can range from planning an event years in advance to planning to carry out the act immediately after passing through screening. The consequences to the actor (perceived as either positive or negative) can range from none to being temporarily detained to deportation, prison, or death.

The FAST research seeks to (1) identify and validate indicators of malintent; (2) develop a prototype incorporating sensors that measure these indicators; and (3) test the performance of the

prototype using volunteers. During the experimental research, the volunteer participant (as notified during the informed consent process) may be explicitly instructed to carry out a disruptive act, so that the researchers and the participant (but not the experimental screeners) already know that the participant has malintent. So in the experimental setting, these three factors would be known (i.e., the participant is told the time horizon, the extent of harm, and the consequences).

The DHS S&T Directorate sponsors the FAST Project, and research laboratories under contract with S&T are conducting the research. The Directors of Research at those laboratories have ultimate control over the design and execution of the FAST research. S&T's role is limited to program management and oversight. This PIA covers the research phase of the FAST project. The project involves conducting research to select the specific sensors that will capture video images, audio recordings, cardiovascular signals, pheromones, electrodermal activity, and respiratory measurements. For example, one potential measurement is heart rate. There are a number of technologies that a sensor can use to capture heart rate. One aspect of the research is determining which specific sensor technology most accurately captures the desired measurement. Another aspect is reviewing the research records to determine if the measurement being captured is actually an indicator of the behavior being evaluated (i.e., did increased heart rate actually occur when the subject was intending to cause a disturbance). In this experimental setting, the participant may be told to cause a disturbance and the sensors would observe the physiological indicators to see if the physiological characteristics reflect that existing intent.

This PIA refers to these two aspects together as "validation" of the sensors. Because this effort involves new applications of technology and related theories, such validation has not yet occurred. The research also entails trying different combinations of sensors to determine which combination works together best.

An Institutional Review Board (IRB) assessed the current research methodology to ensure that the rights, welfare, and privacy of participants in the screening experiments are protected. The IRB also ensures compliance with the human subjects protection requirements set forth in 45 CFR 46, which requires adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data [§46.111(a)(7)]. The project team prepared and coordinated human research subject applications and IRB reviews, including the development of an informed consent form (see Appendix) and protocols for IRB approval prior to testing and screening experiment events. This research effort only involves volunteer participants who understand the experiment and have consented to the specific collections of information through an informed consent process. Throughout the project, project managers will anonymize the data collected, using a unique anonymous identifier rather than participants' names, to protect the privacy of volunteer participants. The laboratories performing the research have complete control over the conduct of the research and all data collected. DHS S&T does not have access to any personally identifiable information collected for this research effort. An IRB will review and approve all FAST research protocols.

The FAST project is a research effort focused on (1) identifying various sensors that will support DHS's screening processes and (2) on the uses of those sensors with volunteers. Based on malintent theory, there are three basic areas that cover most of the behavioral indicators relevant to FAST research: physiological cues, nonverbal behavioral cues, and paralinguistic (vocally produced sounds, not specific

language or words) cues. FAST researchers are currently verifying and validating five sensor types that can detect these cues:

(1) A remote cardiovascular and respiratory sensor to measure heart rate and respiration, which allows for the calculation of heart rate, heart rate variability, respiration rate, and respiratory sinus arrhythmia.

(2) A remote eye tracker, which is a device that uses a camera and processing software to track the position and gaze of the eyes (and, in some instances, the entire head) of a subject. Most eye trackers will also provide a measurement of the pupil diameter.

(3) Thermal cameras that provide detailed information on the changes in the thermal properties of the skin in the face will help assess electrodermal activity and measure respiration and eye movements.

(4) A high resolution video that allows for highly detailed images of the face and body to be taken so that image analysis can determine facial features and expressions and body movements, and an audio system for analyzing human voice for pitch change.

(5) Other sensor types such as for pheromones detection are also under consideration.

Before FAST is transitioned from a research effort to pilot or full deployment in operational environments, the operational component acquiring the technology, with support from S&T, will address the following privacy issues: (1) the legal assessment at Federal, State, and local levels regarding collecting each type of data from each sensor (and combinations of sensors) in an operational setting versus in a research setting with volunteer participants who have consented to the collection; (2) redress options for individuals being screened using the FAST technologies; and (3) data retention limits related to the data collected through FAST technologies.

Under Subchapter 3 §182 of the Homeland Security Act, the Science & Technology Directorate is charged with "conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department." S&T is sponsoring this research in accordance with that mission to support screening activities conducted by DHS Components.

Section 1.0 Information Collected and Maintained

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

1.1 What information is to be collected?

This project is a research and development activity using volunteer participants to test the effectiveness of new screening technologies. The laboratories performing the research collect and hold all information related to the FAST project. DHS S&T only has access to aggregated and anonymized data. Participants who volunteer to take part in the screening experiments provide baseline demographic information that enables researchers to measure FAST's performance across different groups (e.g., whether the technology performs better with specific age groups). The baseline information requested

includes: demographic information (age, gender, occupation, and ethnicity), medical and psychiatric information (heart, circulation, respiratory, vision issues, and treatment for emotional/psychiatric difficulties), current medications, and substance use in the last week (caffeine, tobacco, alcohol, other substances). The demographic information enables the researchers to understand whether the technology performs differently with different demographic groups. The medical/psychiatric information and medication/substance use data allow the researchers to identify factors that may cause the subject to respond differently (e.g., caffeine and nicotine increase the heart rate).

The FAST system will ultimately use non-intrusive sensors (i.e., sensors that collect data without requiring physical contact) to collect video images, audio recordings, and psychophysiological measurements (i.e., heart rate, breathing pattern, eye movement, and electrodermal activity) from the volunteers. (In the preliminary stages of laboratory testing, researchers will use sensors that make physical contact with the volunteer participant in order to ensure that the non-intrusive sensors are accurately collecting data.) Project methodology is subject to a thorough review by the IRB, as discussed above. Researchers will obtain advance informed consent outlining the information to be collected and the research methodology from all participants (see Appendix).

Researchers will assign each participant a unique anonymous identifier for the testing process. This identifier is not based on any piece of data that is linkable to the individual (such as date of birth). All personally identifiable information (PII) collected from the individual (including both the data gathered by the demographics questionnaire and the data gathered by the FAST technology's sensors) is stored under that anonymous identifier. The master list linking names to identifiers is stored in a locked cabinet and accessible only to the laboratory Director of Research. DHS S&T does not have access to the information collected from individuals, only to the aggregated performance data. DHS performs a program management and oversight role but will not be directly involved in performing the research or collecting the data.

Participants may withdraw from the study at any time or decline to provide any information without penalty. If a participant elects to withdraw from the study, the individual may request that all electronic data (including audio and video recordings) pertaining to that individual be destroyed.

1.2 From whom is information collected?

Researchers are collecting information directly from participants who volunteer to participate in the testing and evaluation process. Participants are fully informed of the research methodology prior to entering the experiment (see Appendix). Researchers are currently conducting testing at laboratories under contract with S&T.

Researchers recruit participants through three primary sources:

- Media sources - from newspaper advertisements, pamphlets, or flyer mechanisms;
- Referral sources - from individuals who are aware of or completed the study and inform other individuals who might meet eligibility criteria. These referral sources would provide information (such as a flyer) to potential participants and then allow the potential participants to decide whether to contact research staff;

1.3 Why is the information being collected?

The laboratories are collecting the information gathered by the baseline questionnaires and the FAST sensors in order to evaluate the performance of the FAST technology. Researchers collect the demographic and other baseline information to assess the performance of the FAST technology across different groups (e.g., whether the technology performs better with specific age groups). Researchers use the information collected by the sensors to test the performance of the sensor selection and refine that selection (some types of sensors may work better than others) in order to support the decision-making processes of screeners at transportation and other critical checkpoints.

1.4 How is the information collected?

Volunteers will provide baseline demographic and other information using questionnaires developed by the laboratory research team. During the experiment, sensors will collect video images, audio recordings, and psychophysiological measurements.

1.5 What specific legal authorities/arrangements/agreements define 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. As noted above, the FAST project will be reviewed by an Institutional Review Board that will ensure that the rights, welfare, and privacy of participants in the screening experiments are protected and ensure compliance with the human subjects protection requirements set forth in 45 CFR 46, which require adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data [§46.111(a)(7)].

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

This project is an R&D activity intended to test the effectiveness of an experimental technology. Researchers collect PII (demographic information, video images, and audio recordings) voluntarily with the full advance informed consent of all participants (see Appendix). The potential risk to the individual would be the disclosure of personally identifiable information, such as demographic information, medical information, or video images. To mitigate this risk, all information is anonymized and stored under a unique identifier rather than the person's name.

Researchers assign the information collected (demographic data, video images, audio recordings, and psychophysiological measurements) an anonymous identifier, which can identify research records.

The anonymous identifier is a code number, which is not based on any information that could be used to identify participants. The master list linking names to code numbers is stored separately from the research data in a locked file by the laboratory Director of Research. All data on computers are stored separately from the identifiers and are password protected and limited to authorized laboratory research personnel. Participants' identities are not revealed in any reports or publications resulting from this study. Only authorized research staff have access to the information gathered in this study.

Only the laboratory Director of Research has access to the key linking names to unique identifiers. Hard copies of the informed consent forms signed by the participant are stored in a locked cabinet, and electronic files containing PII (demographic data, medical information, video images, and audio recordings) are password-protected with restricted access. Researchers use all collected information solely for the purpose of conducting ongoing research and development on the FAST technology. The disclosure of any PII (such as video image or audio recording) to anyone outside the laboratory research team will not occur without the express advance written consent of the individual.

Section 2.0 Uses of the System and 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.

Researchers use the information collected to evaluate the performance of the FAST technology in a series of experiments conducted at two laboratories under contract with S&T. Sensors must accurately measure physiological events (heart rate, respiration, etc) and produce signals that data analysis algorithms can process to provide usable data. Researchers have taken an incremental approach to sensor validation, validating each sensor as a standalone sensor and as a component of a larger integrated suite of sensors. The research protocols are developed and executed to measure specific psychophysiological responses. The responses the sensors identify would be presented to screening professionals so those professionals could determine whether the responses indicate malintent (the desire to cause harm). The laboratory research team will use the information from the FAST evaluations to determine how well a particular sensor is functioning and providing the requisite signals. In addition, the research time will assess the pros and cons of deploying that sensor in a location that must accommodate a large number of persons. The ability to measure successfully specific signals in a non-invasive/non-contact manner and in a real-time, high throughput environment is the key discriminator. The project's purpose is to determine the ultimate operational suitability of specific sensors or combinations of sensors for deployment by security officials in environments such as special events, mass transit portals, and border crossings. The project only uses PII from individuals who volunteer to participate.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

The system does not analyze data to identify patterns. However, the technology uses extraction algorithms to identify and analyze specific physiological and/or behavioral cues in order to identify the behaviors being measured and test the overall detection theory.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Participants provide all information voluntarily with their full informed consent. Participants directly provide baseline demographic and other information to enable researchers to measure the performance of FAST across different groups. There is no cross-referencing of any data and no additional check for accuracy for that self-provided data. Sensors also collect information (video images, audio recordings, and psychophysiological measurements). Researchers check sensors for accuracy prior to experimental use by conducting laboratory tests. Once researchers confirm sensor accuracy in the laboratory, no further accuracy checks occur during the field test.

No information collected or used for this research effort will be used for any other purpose.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Access to the information is restricted to the laboratory research team. DHS S&T does not have access to the information collected from study participants; S&T only has access to aggregated performance data. The information (baseline demographic information, video images, audio recordings, and psychophysiological measurements) is stored by an anonymous identifier (rather than by an individual's name) in order to prevent linking data to a specific individual. Physical and computer safeguards are in place to prevent unauthorized persons from gaining access to the data or using it for any purpose other than evaluation and development of the FAST technology.

Physical security for the FAST Laboratory facilities includes an alarm system to secure unattended storage. The security system includes standard security sensors, such as glass break and motion sensors, to detect unauthorized access. In the event of an alarm condition, an automated alert will disseminate via cell phone.

The sensor network, which holds all of the collected information, is a private computer network. Prior to the initiation of data collection, there may be a need to connect the sensor network to the Contractor's network in order to perform sensor validation and system integration tasks and ensure proper sensor/system operation and calibration. This is part of the normal system installation/initiation process and occurs prior to any data collection. The Contractor's network has external connectivity to the Internet but has firewall protection to prevent intrusions. Once data collection has commenced, the sensor network

will not keep an external network connection, therefore making remote attempts to access the data unsuccessful. The network physically exists within the development laboratory and within the modules when installed as a system.

Computer safeguards include password protection, firewalls, auditing tools, and encryption. The operating system logs unauthorized attempts to access the network (such as trying to log in using a non-existent username and password or an incorrect password) on the specific host computer. This log is available to the network administrator for review to audit the login attempts. Data that contains personally identifiable information (e.g., name, birth date, phone number, address) will be encrypted, especially the list that links individuals to their anonymous identifiers. However, it is unnecessary to encrypt the larger research file because no personally identifying information is included and the data is not accessible from a remote network. Physical access to the data is limited to those with access to the laboratory facility and/or module when installed in an operational environment. Only laboratory personnel with proper credentials and passwords and a need to know have access to the system.

Section 3.0 Retention

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

3.1 What is the retention period for the data in the system?

Researchers are collecting information for the purposes of identifying and testing the performance of specific sensors for the FAST technology as well as testing the performance of the technology across different demographic groups. Personally identifiable information (PII) will be retained only as long as it is necessary to support the research and development effort. Researchers will destroy all PII when sensor selection and FAST performance testing has concluded.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No. The S&T Records officer reviewed the project and determined that a retention schedule is not required because the government (i.e., S&T) will not have access to or retain the information collected by researchers.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Data will be retained until researchers can document results and prepare required reports upon completion of evaluations and screening experiments and as required by Institutional Review Board processes. Destruction of data prior to these tasks may invalidate experiment results. For information that

needs retention for research purposes, researchers will store the data either in a locked cabinet (paper documents) or in an access-controlled, password-protected system (electronic files).

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 organizations is the information shared?

Only the aggregated results (e.g., "FAST's performance was accurate XX% of the time in Experiment 1") of the research are shared with S&T. These aggregated results may also be shared with Components of DHS that might choose to acquire the FAST technology for operational use, such as the Transportation Security Agency, Immigration Customs Enforcement, Customs and Border Protection, Secret Service, and Federal Air Marshal Service.

During the testing process, laboratory and other organizational personnel present at the test screening site may incidentally view video images or be exposed to audio tracks as a consequence of being present during the experiments. However, these personnel do not have access to any other PII or know the identity of the participants associated with the images or records. Only the laboratory research team has access to the full set of PII, and then only on a limited, need-to-know basis.

4.2 For each organization, what information is shared and for what purpose?

S&T will share aggregated results with DHS components that may be potential recipients/ customers for this technology to enable them to determine whether FAST would be a useful tool in their operational contexts. Since this is an Innovation project, it is not responding directly to identified homeland capabilities. Rather, the project addresses DHS component gaps--specifically, the need to increase the ability to accomplish people screening within a security context. During the testing process, laboratory personnel may incidentally view video or thermal images or hear audio tracks. However, these personnel do not have access to any personal data. All laboratory personnel who are involved with the laboratory testing or demonstrations have signed prior agreements to treat all PII as restricted information.

4.3 How is the information transmitted or disclosed?

PII is not transmitted or disclosed during the FAST project. However, during the testing process, laboratory personnel may incidentally view video images or be exposed to audio records if present during the experiments. However, these personnel do not have access to any personal data. All laboratory personnel who are involved with the research have completed training on protecting human research participants and have signed agreements to treat all PII as restricted information.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Only the aggregated results (e.g., "FAST's performance was accurate XX% of the time in Experiment 1") of the research are shared with S&T. These aggregated results may also be shared with Components of DHS that might choose to acquire the FAST technology for operational use, such as the Transportation Security Agency, Immigration Customs Enforcement, Customs and Border Protection, Secret Service, and Federal Air Marshal Service. Laboratory and other organizational personnel present during experiments may be incidentally exposed to video images or audio tracks. To mitigate this risk, no personnel outside the immediate laboratory research team have access to any stored PII. All PII (demographic information, video images, audio recordings, and psychophysiological measurements) is stored by anonymized identifier and password-protected.

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 organizations is the information shared?

Researchers share no information with external organizations other than anonymized aggregate results in official test reports. Exposure to video images or audio tracks may occur if other organizations are present during the experiment. PII is not shared with or made available to anyone outside the laboratory research team.

5.2 What information is shared and for what purpose?

No information is shared with external organizations other than anonymized aggregate results in official test reports.

5.3 How is the information transmitted or disclosed?

No information is shared with external organizations other than anonymized aggregate results in official test reports.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Individual Memoranda of Understanding may be developed with external organizations as required for the conduct of screening experiments, and such memoranda will be subject to appropriate legal and privacy review.

5.5 How is the shared information secured by the recipient?

No information is shared with external organizations other than anonymized aggregate results in official test reports.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

No users will be from agencies outside of DHS, so no training is required.

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

The potential risk to the individual would be the disclosure of PII to external organizations. To mitigate this risk, no information is shared with anyone outside the laboratory research team other than anonymized aggregate results in official test reports. Exposure to video images or audio tracks may occur if other organizations are present during the experiment. All laboratory personnel who are involved with the laboratory testing or demonstrations have signed prior agreements to treat all PII as restricted information, meaning that users have permission to access only the information that they have an explicit need to know as determined by the laboratory Director of Research. All system users have signed a user agreement, and only authorized team members have access to system resources. The user agreement includes information on the proper handling of the information, including PII, and a user must execute this agreement prior to being given an account on the computer system.

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? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. Individual participants explicitly consent, in writing, to provide the information (baseline demographic information, video images, audio recordings, and psychophysiological measurements) voluntarily, and they receive detailed written notice (informed consent form, see Appendix) of all information to be collected and how the information will be used. Individuals may, at any time, withdraw from the test or decline to provide PII without penalty. If a participant elects to withdraw from the study, the individual may request that all electronic data (including audio and video recordings) pertaining to that individual be destroyed, including any PII associated with that individual.

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

Yes.

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

Yes. The laboratory research team provides notice to, and requires written consent from, individuals at the time the information is collected. The individuals are informed of how the data will be used prior to initiating the screening experiment, and they have the right to consent to those uses of the information. Individuals' participation in the FAST screening experiment program is entirely voluntary. Personal information collected during the test is used only for the purposes described in this document.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Individuals participating in the test receive advance notice of and provide advance consent for all information that is collected and how the information will be used, thus mitigating the risk of information

being collected without proper notice to and consent from individuals. Participation is entirely voluntary. Individuals may decline to provide any requested information, and they may withdraw from the test at any time with no adverse consequences. If a participant decides to withdraw from the study, that participant has the right to require the research laboratory to destroy all data, including all PII, as well as all sensor data (e.g.: audio and video recordings), collected about him or her. Information is used only for the purposes described in this document.

Section 7.0 Individual 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 which allow individuals to gain access to their own information?

Individuals directly provide baseline demographic information to the researchers and expressly consent to participate in the testing process, including the collection of data by the sensors in the FAST technology. If an individual has concerns that his or her baseline information was given incorrectly, he or she can review this information for accuracy. After the laboratory research team obtains sensor information, individuals cannot access it. (The informed consent form notifies individuals of this fact. See Appendix) Providing participants access to the research sensor data could potentially reveal the capabilities and system performance of the FAST technology, which could facilitate the development of countermeasures that render the technology useless.

7.2 What are the procedures for correcting erroneous information?

Individuals provide their own information and receive instructions to check it for accuracy before submission to the research team. If an individual has concerns that he or she gave baseline demographic information incorrectly, he or she can review this information for accuracy. Researchers check sensors for accuracy in the laboratory prior to the test. After the laboratory research team obtains sensor information, individuals cannot access it.

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

The informed consent form notifies individuals that they cannot access data gathered by the sensors during the test. The individuals themselves provide the demographic data, so there is not a procedure for correcting data beyond asking individuals to verify the accuracy of information they provide. If an individual has concerns that he or she gave baseline demographic information incorrectly, he or she can review this information for accuracy. However, the individual is not allowed to review his audio, video, or psychophysiological recordings.

7.4 If no redress is provided, are alternatives available?

Yes. The individual is free to leave the test at any point or to decline to provide information. If a participant decides to withdraw from the study, that participant has the right to require the laboratory to destroy all data (including PII, and audio and video recordings) collected about him or her.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The individuals are volunteer participants, and the research team obtains their advance informed consent regarding the information to be collected. Other than being allowed to review baseline demographic information for accuracy, additional access, correction, or redress rights are not provided because granting access to the research sensor data could diminish the ultimate operational utility of the technology. Providing participant access to the sensor data could potentially reveal the capabilities and system performance of the FAST technology, which could facilitate the development of countermeasures that render the technology useless.

Section 8.0 Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

User groups are not granted “blanket” access to the system. Rather, access is dependent upon the particular situation. Researchers have documented access requirements in the screening experiment plans. All user groups consist of authorized laboratory personnel, and only personnel with a need to know have access to the data for each scenario-defined data set.

8.2 Will contractors to DHS have access to the system? If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

Yes. The contracted laboratories are the only parties who have access to the system and the data collected. DHS only has access to the aggregated performance data.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Users have permission to access only the information that they have an explicit need to know as determined by the laboratory Director of Research.

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

The decision authority to create accounts and determine access to data rests with the laboratory project director, who ensures that proper permissions are assigned by the systems administrator. The principal investigator for the IRB research studies is ultimately responsible for safeguarding the rights of each participant.

Access privileges to the system are documented using a User Account Authorization form, which is retained by the system administrator.

In addition to the User Account Authorization form, laboratory personnel are required to submit a Non-Disclosure Form.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Each user's access to the system has a timestamp tracking history. The history documents all persons who have viewed, edited, or printed information, and the audit includes the date, time, and location of the user.

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

Systematic network and system monitoring is in place to detect intrusions. Role-based security is used to prevent unauthorized use of the information, including improper printing or editing of data, and a two-person access is required for access to PII.

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

All users receive privacy training prior to their first access to PII related to this project. The privacy training provides an overview of Federal and DHS privacy requirements, as well as privacy concerns specific to the FAST technology. In addition, all laboratory staff have completed human subject protection training, which also addresses the proper handling and protection of PII.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

S&T is following information security practices consistent with the FISMA, but has not initiated the formal C&A process for FAST because the sensors to be used in the project are still in the selection process. Once the sensor suite has been finalized, S&T will consult the Chief Information Officer to determine if C&A is required.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Security controls are in place to protect the confidentiality, availability, and integrity of the data, including role-based access controls that enforce a strict need-to-know policy. Each user receives a unique login name and password, and audit trails are maintained and regularly checked to track user access and detect any unauthorized use. All system users have signed a user agreement, and only authorized team members have access to system resources. The user agreement includes information on the proper handling of sensitive information, including PII, and a user must execute this agreement prior to being given an account on the computer system. All users have completed the Human Participants Education for Research Teams and are familiar with the proper procedures for handling sensitive information. Team members who do not need access to the systems were not given logon accounts. The use of the system is for project related work only. Personal use and other non-project use of the system is not permitted. In addition, all laboratory personnel granted access to the FAST system have signed a Non-Disclosure Agreement and agreed to treat all PII information as confidential.

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 Was the system built from the ground up or purchased and installed?

The system is being built from the ground up.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

In addition to the process to anonymize data identified in paragraph 8.9, the following technical safeguards are in place to secure data:

- Use of advanced encryption technology to prevent internal and external inadvertent disclosure

- Secure data transmission, including the use of password-protected e-mail for sending files containing sensitive information to prevent unauthorized access
- Password protection for files to prevent unauthorized access
- Network firewalls to prevent intrusion into network and databases
- User identification and password authentication to prevent access by unauthorized users
- Security auditing tools to identify the source of failed system access attempts by unauthorized users and the improper use of data by authorized operators
- Vulnerability assessments, risk analysis, and process auditing to ensure compliance with applicable federal policies and procedures and federal automated information systems requirements
- Restricting access to the system to only those laboratory personnel with a strict need to know and appropriate clearances. All individuals with access to the system who interact with test subjects have completed human subjects protection training.

9.3 What design choices were made to enhance privacy?

In addition to the safeguards identified in paragraph 8.9, access to the system is strictly controlled and limited according to the individual's need to know the information to perform their duties. As noted above, systematic network and system monitoring is in place to detect intrusions. Each login to the system has a timestamp tracking history listing what has been viewed, edited, or printed, and the timestamp includes the date, time and location of the user. All information in the system is secured in accordance with Federal standards. The system was designed to include firewalls, audit trails, password protection, and two-person access to PII in order to enhance privacy protection.

Conclusion

In every aspect of this work, the program shall provide for appropriate privacy protection and ensure sufficient information is provided to research personnel to improve user experience and throughput, provide automated behavior based screening techniques, integrate multiple screening technology systems, validate technical requirements analysis, and establish performance metrics for screening systems. If successful, the components developed through this research effort would be offered as generic functional elements that could be considered for operational use by DHS operational components.

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

APPENDIX

For a copy of the appendixes, please email PIA@dhs.gov