U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Investigations & Oversight

HEARING CHARTER

Behavioral Science and Security: Evaluating TSA's SPOT Program

Wednesday, April 6, 2011
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

The Subcommittee on Investigations and Oversight meets on April 6, 2011 to examine the Transportation Security Administration's (TSA) efforts to incorporate behavioral science into its transportation security architecture. The Department of Homeland Security (DHS) has been criticized for failing to scientifically validate the Screening of Passengers by Observational Techniques (SPOT) program before operationally deploying it. SPOT is a TSA program that employs Behavioral Detection Officers (BDO) at airport terminals for the purpose of detecting behavioral based indicators of threats to aviation security.

The hearing will examine the state of behavioral science as it relates to the detection of terrorist threats to the air transportation system, as well as its utility to identify criminal offenses more broadly. The hearing will examine several independent reports—one by the Government Accountability Office (GAO), two by the National Research Council, and a number of Defense and Intelligence Community advisory board reports on the state of behavioral science relative to the detection of emotion, deceit, and intent in controlled laboratory settings, as well as in an operational environment. The Subcommittee will evaluate the initial development of the SPOT program, the steps taken to validate the science that form the foundation of the program, as well as the capabilities and limitations of using behavioral science in a transportation setting. More broadly, the hearing will also explore the behavioral science research efforts throughout DHS.

Background

The terrorist attacks on September 11, 2001 exposed a vulnerability in the nation's air transportation system. In order to augment other screening processes and procedures, TSA conducted operational testing of behavior detection techniques at a limited number of airports in October 2003.[1] In 2007, TSA created new BDO positions as part of the SPOT program with the goal of identifying persons who may pose a potential security risk by using behavioral indicators such as stress, fear, or deception.[2]

[1] Aviation Security: Efforts to validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges, Government Accountability Office, May 2010. Available at http://www.gao.gov/new.items/d10763.pdf
[2] *Ibid.*

The indicators BDOs use form a checklist with corresponding values and thresholds. These indicators, values, and thresholds are used to assess passengers while in line awaiting security screening. When an individual displays behaviors or an appearance that exceeds a predetermined threshold, they are referred for additional screening. If, during the course of this secondary screening, individuals display behaviors that exceed another threshold, they are referred to law enforcements officers for further investigation.

Initially established to detect terrorist threats to the aviation transportation system,[3] the program's mission has since broadened to include the identification of behaviors indicative of criminal activity.[4] Critics of the program have argued that this expansion reflects the failure of the program to identify any terrorists, and therefore program success could only be quantified by broadening the goals to include criminal activity which has a higher rate of occurrence.[5] This may or may not be a fair critique based on the extremely small sample size that terrorists would represent. Regardless of the rationale for the program's expanded scope, questions remain about whether indicators for terrorism are the same for criminal behavior.

As of March 2010, TSA employed roughly 3000 BDOs at approximately 161 airports at a cost of $212 million a year.[6] In the President's fiscal year 2012 budget request, the Department seeks to add 175 more BDOs with an increase of $21 million – a 9.5 % increase over current funding levels.[7] In total, the five year budget profile for the SPOT program accounts for roughly $1.2 billion.[8]

Relevant Reviews

U.S. Government Accountability Office (GAO)
Aviation Security: Efforts to validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges

In May 2010, GAO issued a report titled "Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges" in response to a Congressional request to review the SPOT program. In preparing the report, GAO analyzed "(1) the extent to which TSA validated the SPOT program before deployment, (2) implementation challenges, and (3) the extent to which TSA measures SPOT's effect on aviation security."[9]

GAO issued the following findings associated with its review:

[3] *Ibid.*
[4] Congressional Budget Justification FY2012, Department of Homeland Security.
[5] Weinberger, Sharon, "Intent to Deceive? Can the Science of Deception Detection Help to Catch Terrorists?" *Nature*, Vol. 465127, May 26, 2010, available at: http://www.nature.com/news/2010/100526/pdf/465412a.pdf
[6] S*upra* n.1.
[7] S*upra* n.4.
[8] S*upra* n.1.
[9] *Ibid*.

Although the Department of Homeland Security (DHS) is in the process of validating some aspects of the SPOT program, TSA deployed SPOT nationwide without first validating the scientific basis for identifying suspicious passengers in an airport environment. A scientific consensus does not exist on whether behavior detection principles can be reliably used for counterterrorism purposes, according to the National Research Council of the National Academy of Sciences. According to TSA, no other large-scale security screening program based on behavioral indicators has ever been rigorously scientifically validated. DHS plans to review aspects of SPOT, such as whether the program is more effective at identifying threats than random screening. Nonetheless, DHS's current plan to assess SPOT is not designed to fully validate whether behavior detection can be used to reliably identify individuals in an airport environment who pose a security risk. For example, factors such as the length of time BDOs can observe passengers without becoming fatigued are not part of the plan and could provide additional information on the extent to which SPOT can be effectively implemented. Prior GAO work has found that independent expert review panels can provide comprehensive, objective reviews of complex issues. Use of such a panel to review DHS's methodology could help ensure a rigorous, scientific validation of SPOT, helping provide more assurance that SPOT is fulfilling its mission to strengthen aviation security.[10]

Additionally, GAO found issues relating to performance metrics, data integrity, and reach-back capabilities as well.

TSA is experiencing implementation challenges, including not fully utilizing the resources it has available to systematically collect and analyze the information obtained by BDOs on passengers who may pose a threat to the aviation system. TSA's Transportation System Operations Center has the resources to investigate aviation threats but generally does not check all law enforcement and intelligence databases available to it to identify persons referred by BDOs. Utilizing existing resources would enhance TSA's ability to quickly verify passenger identity and could help TSA to more reliably "connect the dots." Further, most BDOs lack a mechanism to input data on suspicious passengers into a database used by TSA analysts and also lack a means to obtain information from the Transportation System Operations Center on a timely basis. TSA states that it is in the process of providing input capabilities, but does not have a time frame for when this will occur at all SPOT airports. Providing BDOs, or other TSA personnel, with these capabilities could help TSA "connect the dots" to identify potential threats.

Although TSA has some performance measures related to SPOT, it lacks outcome-oriented measures to evaluate the program's progress toward reaching its goals. Establishing a plan to develop these measures could better position TSA to determine if SPOT is contributing to TSA's strategic goals for aviation security. TSA is planning to enhance its evaluation capabilities in 2010 to more readily assess the program's effectiveness by conducting statistical analysis of data related to SPOT referrals to law enforcement and associated arrests.[11]

Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue

In March of 2011, GAO issued a report to Congress in response to a new statutory requirement that GAO identify federal programs, agencies, offices, and initiatives, either within departments or governmentwide, which have duplicative goals or activities. The report contained a section on SPOT and stated:

[10] *Ibid.*
[11] *Ibid.*

Congress may wish to consider limiting program funding pending receipt of an independent assessment of TSA's SPOT program. GAO identified potential budget savings of about $20 million per year if funding were frozen at current levels until validation efforts are complete. Specifically, in the near term, Congress could consider freezing appropriation levels for the SPOT program at the 2010 level until the validation effort is completed. Assuming that TSA is planning to expand the program at a similar rate each year, this action could result in possible savings of about $20 million per year, since TSA is seeking about a $20 million increase for SPOT in fiscal year 2011. Upon completion of the validation effort, Congress may also wish to consider the study's results—including the program's effectiveness in using behavior-based screening techniques to detect terrorists in the aviation environment—in making future funding decisions regarding the program.[12]

Credibility Assessment at Portals Report

In April 2009, the Portals Committee issued a report for the Defense Academy for Credibility Assessment titled: "Credibility Assessment at Portals."[13] The committee recognized the need for "advanced and accurate credibility assessment,"[14] which is described as "a decision making process whereby a communication is assessed as to its veracity." The Portals Committee had the following to say about SPOT:

"The adoption of SPOT occurred despite the fact that no study in the peer-reviewed scientific literature suggests that accurate credibility assessments can be made from unstructured observations. Within SPOT it appears that the observers are attempting to assess airline passengers by casual observation of facial micro-expressions (Wilber & Nakashima, 2007). There are several problems with this. First, scientific research does not support the notion that microexpressions reliably betray concealed emotion (Porter & ten Brinke, 2008). Second, whereas brief facial activity may reveal the purposeful manipulation of a felt emotion (Porter & ten Brinke, 2008), the problems of interpretation of such manipulation renders the approach useless for practical purposes. Third, the microexpression approach equates deception with manipulated emotion. This conceptual confusion obscures the fact that most forensically relevant lies are not lies about feelings but about actions in the past, present or future. In conclusion, the use of microexpressions to establish credibility is theoretically flawed and has not been supported by sound scientific research (Vrij, 2008)."[15]

JASON

Comprised of world renowned scientists, JASON advises the federal government on science and technology issues. The vast majority of its work is done at the request of the Department of Defense and the intelligence community, so its reports are typically classified.

However, a 2010 *Nature* article that discusses the SPOT program in a piece on deception detection provides the following: "'No scientific evidence exists to support the detection or

[12] Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue, Government Accountability Office, March 2011, available at: http://www.gao.gov/new.items/d11318sp.pdf

[13] "Credibility Assessment at Portals," Portals Committee Report, April 17, 2009, available at: http://truth.boisestate.edu/eyesonly/Portals/PortalsCommitteeReport.pdf

[14] *Ibid.*

[15] *Ibid.*

inference of future behaviour, including intent,' declares a 2008 report prepared by the JASON defence advisory group."[16]

National Research Council (NRC) of the National Academies

Workshop Summary on *Field Evaluation in the Intelligence and Counterintelligence Context*

On September 22-23, 2009, the NRC's Board on Behavioral, Cognitive, and Sensory Sciences held a workshop on "the field evaluation of behavioral and cognitive sciences-based methods and tools for use in the areas of intelligence and counter intelligence."[17] The workshop was sponsored by the Defense Intelligence Agency and the Office of the Director of National Intelligence. The purpose of the workshop was to "discuss the best ways to take methods and tools from behavioral science and apply them to work in intelligence operations. More specifically, the workshop focused on the issue of field evaluation – the testing of these methods and tools in the context in which they will be used in order to determine if they are effective in real world settings."[18]

The NRC published a report in 2010 summarizing the presentations and discussions over the 2-day period. Participants of the workshop included NRC members and experts in the behavioral sciences and intelligence community. The goal of the workshop was "not to provide specific recommendations but to offer some insight – in large part through specific examples taken from other fields – into the sorts of issues that surround the area of field evaluations. The discussions covered such ground as the obstacles to field evaluation of behavioral science tools and methods, the importance of field evaluation, and various lessons learned from experience with field evaluation in other areas."[19]

While the report identified several obstacles, one of interest to this Subcommittee hearing is "the pressure to use new devices and techniques as soon as they become available, without waiting for rigorous validation. Because lives are at stake, those in the field often push to adopt new methods and tools as quickly as possible and before there has been time to evaluate them adequately. Once a method is in widespread use, anecdotal evidence can lead its users to believe in its effectiveness and to resist rigorous testing, which may show that it's not as effective as they think."[20]

Protecting Individual Privacy in the Struggle Against Terrorists – A Framework for Program Assessment

---

[16] *Supra n.5.*
[17] "Field Evaluation in the Intelligence and Counterintelligence Context," National Research Council of the National Academies , 2010, available at: http://books.nap.edu/openbook.php?record_id=12854&page=R1
[18] *Ibid.*
[19] *Ibid.*
[20] "Field Evaluation in the Intelligence and Counterintelligence Context," National Research Council of the National Academies, March 2010, available at: http://www7.nationalacademies.org/bbcss/Highlights-Field%20Evaluation%20in%20the%20Intelligence%20and%20Counterintelligence%20Context.pdf

From 2005 to 2007, the NRC's 21-member Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals held several meetings to "examine the role of data mining and behavioral surveillance technologies in counterterrorism programs."[21] The ensuing NRC report provides "a framework for making decisions about deploying and evaluating those [programs] and other information based programs on the basis of their effectiveness and associated risks to personal privacy."[22]

The report presented 13 conclusions and 2 broad recommendations. Of interest to this Subcommittee hearing are the following conclusions:

- *"Conclusion 3: Inferences about intent and/or state of mind implicate privacy issues to a much greater degree than do assessments or determinations of capability.*

  Although it is true that capability and intent are both needed to pose a real threat, determining intent on the basis of external indicators is inherently a much more subjective enterprise than determining capability. Determining intent or state of mind is inherently an inferential process, usually based on indicators such as whom one talks to, what organizations one belongs to or supports, or what one reads or searches for online. Assessing capability is based on such indicators as purchase or other acquisition of suspect items, training, and so on. Recognizing that the distinction between capability and intent is sometimes unclear, it is nevertheless true that placing people under suspicion because of their associations and intellectual explorations is a step toward abhorrent government behavior, such as guilt by association and thought crime. This does not mean that government authorities should be categorically proscribed from examining indicators of intent under all circumstances—only that special precautions should be taken when such examination is deemed necessary."

- *"Conclusion 4: Program deployment and use must be based on criteria more demanding than 'it's better than doing nothing.'*

  In the aftermath of a disaster or terrorist incident, policy makers come under intense political pressure to respond with measures intended to prevent the event from occurring again. The policy impulse to do something (by which is usually meant something new) under these circumstances is understandable, but it is simply not true that doing something new is always better than doing nothing. Indeed, policy makers may deploy new information-based programs hastily, without a full consideration of (a) the actual usefulness of the program in distinguishing people or characteristic patterns of interest for follow-up from those not of interest, (b) an assessment of the potential privacy impacts resulting from the use of the program, (c) the procedures and processes of the organization that will use the program, and (d) countermeasures that terrorists might use to foil the program.

- *"Conclusion 10: Behavioral and physiological monitoring techniques might be able to play an important role in counterterrorism efforts when used to detect (a) anomalous states (individuals whose behavior and physiological states deviate from norms for a particular situation) and (b) patterns of activity with well-established links to underlying psychological states.*

[21] "Protecting Individual Privacy in the Struggle against Terrorists – A Framework for Program Assessment," National Research Council of the National Academies, 2008, available at: http://books.nap.edu/openbook.php?record_id=12452&page=1

[22] *Ibid*.

Scientific support for linkages between behavioral and physiological markers and mental state is strongest for elementary states (simple emotions, attentional processes, states of arousal, and cognitive processes), weak for more complex states (deception), and nonexistent for highly complex states (terrorist intent and beliefs). The status of the scientific evidence, the risk of false positives, and vulnerability to countermeasures argue for behavioral observation and physiological monitoring to be used at most as a preliminary screening method for identifying individuals who merit additional follow-up investigation. Indeed, there is no consensus in the relevant scientific community nor on the committee regarding whether any behavioral surveillance or physiological monitoring techniques are ready for use at all in the counterterrorist context given the present state of the science."

- *"Conclusion 11: Further research is warranted for the laboratory development and refinement of methods for automated, remote, and rapid assessment of behavioral and physiological states that are anomalous for particular situations and for those that have well-established links to psychological states relevant to terrorist intent.*

  A number of techniques have been proposed for the machine-assisted detection of certain behavioral and physiological states. For example, advances in magnetic resonance imaging (MRI), electroencephalography (EEG), and other modern techniques have enabled measures of changes in brain activity associated with thoughts, feelings, and behaviors. Research in image analysis has yielded improvements in machine recognition of faces under a variety of circumstances (e.g., when a face is smiling or when it is frowning) and environments (e.g., in some nonlaboratory settings).

  However, most of the work is still in the basic research stage, with much of the underlying science still to be validated or determined. If realworld utility of these techniques is to be realized, a number of issues— practical, technical, and fundamental—will have to be addressed, such as the limits to understanding, the largely unknown measurement validity of new technologies, the lack of standardization in the field, and the vulnerability to countermeasures. Public acceptability regarding the privacy implications of such techniques also remains to be demonstrated, especially if the resulting data are stored for unknown future uses or undefined lengths of time.

  For example, the current state-of-the-art of functional MRI technology can identify changes in the hemodynamics in certain regions of the brain, thus signaling activity in those regions. But such results are not necessarily consistent across individuals (i.e., different areas in the brains of different individuals may be active under the same stimulus) or even in the same individual (i.e., a slightly different part of the brain may become active even in the same individual under the same stimulus). Certain regions of the brain may be active under a variety of different stimuli.

  In short, understanding of what these regions do is still primitive. Furthermore, even if simple associations can be made reliably in laboratory settings, this does not necessarily translate into usable technology in less controlled situations. Behavior of interest to detect, such as terrorist intent, occurs in an environment that is very different from the highly controlled behavioral science laboratory."

- *"Conclusion 12: Technologies and techniques for behavioral observation have enormous potential for violating the reasonable expectations of privacy of individuals.*

  Because the inferential chain from behavioral observation to possible adverse judgment is both probabilistic and long, behavioral observation has enormous potential for violating the reasonable expectations of privacy of individuals. It would not be unreasonable to suppose that most individuals would be far less bothered and concerned by searches aimed at finding tangible objects that might be weapons or by queries aimed at authenticating their identity than by technologies and techniques whose use will inevitably force targeted individuals to explain and

justify their mental and emotional states. Even if behavioral observation and physiological monitoring are used only as a preliminary screening methods for identifying individuals who merit additional follow-up investigation, Because the inferential chain from behavioral observation to possible adverse judgment is both probabilistic and long, behavioral observation has enormous potential for violating the reasonable expectations of privacy of individuals. It would not be unreasonable to suppose that most individuals would be far less bothered and concerned by searches aimed at finding tangible objects that might be weapons or by queries aimed at authenticating their identity than by technologies and techniques whose use will inevitably force targeted individuals to explain and justify their mental and emotional states. Even if behavioral observation and physiological monitoring are used only as a preliminary screening methods for identifying individuals who merit additional follow-up investigation, these individuals will be subject to suspicion that would not fall on others not so identified."[23]

Issues

Detection of Emotion

The state of science relative to the detection of emotion, deceit, and intent are vastly different. Decades of research have been devoted to the detection of emotion using verbal, nonverbal, and microfacial expressions. Each of these observational techniques have shown to have varying degrees of success at determining an individual's emotion, but generally speaking, a scientific foundation does exist to support the assertion that emotion can be determined through behavioral cues.

Detection of Deceit

The foundation of research for detecting an expression of deceit is rooted in that of emotion. For example, it is posited that a deceitful person would express emotions such as stress, and that stress can be attributed to concealing a lie. The state of the science in this regard is less solid. Witnesses at the hearing will testify to the current strengths and weaknesses of this field.

Detection of Intent

Even less certainty exists regarding the ability to determine intent. This ability is asserted by assuming that a person who intends to do harm will be concealing this fact, thereby expressing deceitful behaviors – and that deceitful behavioral cues are founded in stress, which in turn are displayed in emotion. This chain of reasoning takes the underlying assumption that behavioral indicators exist for detecting emotion and infers that indicators can therefore be used to detect deceit, and therefore intent. Very little, if any, evidence exists in the scientific literature to support this hypothesis, yet this is the goal of the SPOT program - to identify individuals who may pose a threat to aviation security.

Laboratory vs. Operational Settings

The vast preponderance of behavioral science research conducted relative to the detection of emotion, deceit, and intent has been done in a laboratory setting. As the National Research

[23] *Ibid.*

Council noted in its 2008 report, "Behavior of interest to detect, such as terrorist intent, occurs in an environment that is very different from the highly controlled behavioral science laboratory."[24]

Utility for Counterterrorism

Even if one was to stipulate that a body of evidence existed to support the claim that one could detect intent using behavioral indicators, it remains to be seen how useful this would be in a counterterrorism context. In all likelihood, anyone seeking to cause harm would employ countermeasures designed to conceal their emotions. It remains to be seen what impact countermeasures will have on the ability to detect emotions, deception, or intent, but if other deception detection tools (such as the polygraph) are any indicator, they could severely degrade the capability.

Utility in a U.S. Aviation Transportation Setting

The SPOT program is loosely based on the Israeli model successfully employed by El Al Airlines. This highly successful program employs more agents in more locations throughout the airport, conducts multiple face to face interviews, actively profiles passengers, and operates in smaller and fewer airports. They also have much fewer passengers and far fewer flights than the U.S. air transportation system. Israeli screeners also receive more training than the four days of classroom training, and three days of on the job training that BDOs receive. Scaling up such an enterprise to accommodate the U.S. Aviation Transportation Sector would severely restrict the flow of commerce and passengers.

DHS S&T Validation

In its report, GAO states that "TSA deployed SPOT nationwide without first validating the scientific basis for the program."[25] To its credit, DHS S&T initiated a review two and a half years ago to "determine whether SPOT is more effective at identifying passengers who may be threats to the aviation system than random screening."[26] GAO goes on to point out in its report, "However, S&T's current research plan is not designed to fully validate whether behavior detection and appearances can be effectively used to reliably identify individuals in an airport terminal environment who pose a risk to the aviation system."[27] The report further states that, according to the National Research Council, "an independent panel could provide an objective assessment of the methodologies and findings of DHS's study to better ensure that SPOT is based on valid science."[28]

These are two important points. First, the S&T review is not designed to validate the underlying behavioral cues, but rather to simply demonstrate whether the program, as a whole, is more successful than random sampling. As GAO stated in its recent "Duplication" report, "DHS's

[24] *Supra* n.21.
[25] *Supra* n.1.
[26] *Ibid.*
[27] *Ibid.*
[28] *Ibid.*

response to GAO's report did not describe how the review currently planned is designed to determine whether the study's methodology is sufficiently comprehensive to validate the SPOT program."[29] Second, based on the Statement of Work associated with S&T's review, questions remain as to whether or not the review is truly independent.

The Statement of Work affirms that S&T had a direct role in selecting peer reviewers, as well as planning and structuring workshops that informed the methodology to validate the program. The Statement of Work also afforded DHS the ability to review and provide revision recommendations at numerous points in the process. Finally, the Statement of Work indicates that deliverables are to be provided to S&T directly.[30] Whether or not this affected the outcome is uncertain. The validation work was conducted by the American Institute for Research, a high respected and reputable firm, but ultimately they are contractually bound by the parameters and scope defined by Statement of Work negotiated with DHS. It remains to be seen whether the review was an independent assessment, as recommended by the National Research Council, or more of a collaboration.

Nevertheless, S&T's two and a half year review (at a cost of $2.5 million) was initially planned to be delivered in Fiscal year 2011,[31] then February 2011,[32] and then the end of March 2011. Its current release date is for April 8th, two days after our hearing. The Subcommittee postponed this hearing, initially scheduled for March 17th, for a number of reasons, including allowing S&T more time to produce the report.

Witnesses

Mr. Stephen Lord, Director, Homeland Security and Justice Issues, Government Accountability Office

Transportation Security Administration (Invited)

Mr. Larry Willis, Program Manager, Homeland Security Advanced Research Projects Agency, Science and Technology Directorate, Department of Homeland Security

Dr. Paul Ekman, Professor Emeritus of Psychology, University of California, San Francisco, and President and Founder, Paul Ekman Group, LLC

Dr. Maria Hartwig, Associate Professor, Department of Psychology, John Jay College of Criminal Justice

Dr. Philip Rubin, Chief Executive Officer, Haskins Laboratories

---

[29] *Supra* n.12.
[30] Statement of Work for the Naval Research Laboratory, Project Hostile Intent: Behavioral-Based Screening Indicators Validation, U.S. department of Homeland Security, Science and Technology Directorate, Human Factors and Behavioral Sciences Division, PR# RSHF-11-00007.
[31] *Supra* n.1.
[32] *Supra* n.12.

Lieutenant Detective Peter J. DiDomenica, Boston University Police

Appendix 1

Department of Homeland Security
Science and Technology Directorate
Human Factors Behavioral Sciences Projects

These projects advance national security by developing and applying the social, behavioral, and physical sciences to improve identification and analysis of threats, to enhance societal resilience, and to integrate human capabilities into the development of technology.

Commercial Data Sources Project

Project Manager: Patty Wolfhope

Project Overview: The Science and Technology (S&T) Directorate Human Factors Behavior Sciences Division (HFD) Commercial Data Sources Project will quantitatively assess the utility of commercial data sources to augment governmentally available information about people, foreign and domestic, being screened, investigated, or vetted by the Department. The use of commercial data sources may provide a valuable source of corroborating information to ensure that an individual's identity and eligibility for a particular license, privilege, or status is correctly evaluated during screening. This project is part of the Personal Identification Systems Thrust Area and Credentialing Program within HFD.

Community Perceptions of Technology Panel Project

Project Manager: Ji Sun Lee

Project Overview: The Science and Technology (S&T) Directorate Human Factors/ Behavioral Sciences Division (HFD) Community Perceptions of Technology Panel (CPT) Project brings together representatives of industry, public interest, and community-oriented organizations to better understand and integrate community perspectives and concerns in the development, deployment, and public acceptance of technology. This will yield feedback to aid ongoing technology and process development and strategies to accurately inform the public of new approaches to securing the homeland. This is designed to better ensure acceptance of the technology within affected communities. This project is part of the Human Technology Integration Thrust Area and Technology Acceptance and Integration Program within HFD.

Community Resilience Project

Project Manager: Michael Dunaway

Project Overview: The Science and Technology (S&T) Directorate Human Factors/ Behavioral Sciences Division (HFD) Counter-Improvised Explosives Devices (IED) Community Resilience Project conducts research into methodologies for effective hazard and risk communications to enhance the ability of local officials to convey understandable and credible warnings of IED activity to the public. This project will help local government and civic officials understand how to properly frame risk warnings and post-event instructions to the public in a manner that maximizes the public's understanding of the instructions provided and maintains public trust and confidence. HFD is executing this project as part of the Counter Improvised Explosive Devices (C-IED) Thrust Area and Mitigate Program within Explosives Division.

Counter-IED Actionable Indicators and Countermeasures Project

Project Manager: Allison Smith, Ph.D.

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Counter-Improvised Explosives Devices (IED) Actionable Indicators and Countermeasures Project supports the intelligence and law enforcement communities in identifying actors that pose significant IED threats in the United States homeland. This project will provide practical tools through the synthesis of state-of-the-art social and behavioral science databases, case studies, surveys, and fieldwork and advanced computational modeling, simulation, and visualization technologies. It will also provide policymakers with scientifically tested strategies to prevent radicalization and IED attacks before they occur by examining how social and behavioral science principles can support the development of counter-radicalization efforts. HFD is executing this project as part of the Counter Improvised Explosive Devices (C-IED) Thrust Area and Prevent/Deter Program.

Credentialing Project

Project Manager: Patty Wolfhope

Project Overview: The Science and Technology (S&T) Directorate Human Factors Behavior Sciences (HFD) Division Credentialing Project develops tamper-proof credentialing systems that incorporate biometric information; such as a biometrics-based card-and-reader system. The project developed a laboratory test and evaluation protocol for the transportation worker identification card (TWIC) reader and plans to initiate research and design activities to improve the range and reliability of secure contactless technologies. This project is part of the Personal Identification Systems Thrust Area and Credentialing Program within HFD.

Enhanced Screener-Technology Interface Project

Project Manager: Josh Rubinstein, Ph.D.

Project Overview: The Science and Technology (S&T) Directorate Human Factors Behavioral Sciences (HFD) Division Enhanced Screener-Technology Interface Project characterizes screener-performance issues, proposes new screener technologies and procedures, and develops training curricula to optimize security effectiveness and reduce human fatigue and injury, while reducing training requirements and overall cost. This project is part of the Human Technology Integration Thrust Area and Transportation Technology-Human Integration Program within HFD.

Enhancing Public Response and Community Resilience Project

Project Manager: Michael Dunaway

Project Overview: The Science and Technology (S&T) Directorate Human Factors/ Behavioral Sciences Division (HFD) Enhancing Public Response and Community Resilience Project examines public needs (shelter, food, disaster relief, etc.) that arose during the evacuation from southern Texas during Hurricanes Katrina and Rita in order to enhance federal, state, local and private sector response to future catastrophic events. The goal is to capture and communicate lessons learned to enhance federal, state, local and private sector responses to future catastrophic events. This project is part of the Social and Behavioral Threat Analysis (SBTA) Thrust Area and Community Preparedness and Resilience Program within HFD.

High Impact Technological Solution - Biometric Detector Project

Project Manager: Arun Vemury

Project Overview: The Science and Technology (S&T) Directorate High Impact Technological Solutions (HITS) Project executed by the Human Factors/Behavioral Science Division (HFD) will provide efficient, high quality, contact less acquisition of fingerprint biometric signatures for identity management. This will result in significantly improved throughput and signal quality, thereby improving recognition and reducing false positive rates. The goal is to develop a fingerprint acquisition device that can be transitioned for implementation across Department components. This project is part of the Innovations Portfolio/Homeland Security Advanced Research Project Agency Program (HSARPA) within the S&T Directorate.

Homeland Innovation Prototypical Solutions - Future Attribute Screening Technology (FAST) Project

Project Manager: Bob Burns

Project Overview: The Homeland Security Advanced Research Project Agency (HSARPA) and Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Future Attribute Screening Technology (FAST) Project is an initiative to develop innovative, non-invasive technologies to screen people at security checkpoints. FAST is grounded in research on human behavior and psychophysiology, focusing on new advances in behavioral/human-centered screening techniques. The aim is a prototypical mobile suite (FAST M2) that would be used to increase the accuracy and validity of identifying persons with malintent (the intent or desire to cause harm). Identified individuals would then be directed to secondary screening, which would be conducted by authorized personnel. This project is part of the Innovations Portfolio/Homeland Security Advanced Research Project Agency (HSARPA) Program within the S&T Directorate.

Hostile Intent Detection - Automated Prototype Project

Project Manager: Larry Willis

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Hostile Intent Detection - Automated Prototype Project demonstrates real-time automated intent detection using non-invasive and culturally neutral behavioral indicators. S&T plans to transition the automated hostile intent prototype to the Transportation Security Administration, Customs and Border Protection, and Immigration and Customs Enforcement. This project is a part of the Social and Behavioral Threat Analysis Thrust Area and Suspicious Behavior Detection Program within HFD.

Hostile Intent Detection - Training & Simulation Project

Project Manager: Larry Willis

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Hostile Intent Detection – Training and Simulation Project develops computer-based simulation to train behavior-based stand-off detection for future hostile intent using indicators from the interactive screening environment (Hostile Intent Detection – Automated Prototype) and the observational environment (Hostile Intent Detection – Validation) to support screening and interviewing interactions at air, land, and maritime portals. This project is part of the Social and Behavioral Threat Analysis Thrust Area and Suspicious Behavior Detection Program within HFD.

Hostile Intent Detection - Validation Project

Project Manager: Larry Willis

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Hostile Intent Detection – Validation Project provides cross-cultural validation of behavioral indicators employed by Department of Homeland Security's operational components to screen passengers at air, land, and maritime ports. The project will integrate these validated behavioral indicators into the screening curriculum of each component's existing training program. This project is part of the Social and Behavioral Threat Analysis Thrust Area and Suspicious Behavior Detection Program within HFD.

Human Systems Engineering Project

Project Managers: Darren P. Wilson and Janae Lockett-Reynolds, Ph.D.

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Project develops, demonstrates and evaluates a standardized process for implementing human systems integration. It will focus on defining human performance requirements in the development of systems and technology, and on methods and measures needed to evaluate existing technology in terms of human performance requirements. This effort also will result in greater understanding of the needs of the various Department end-user communities, as well as developing tools to best identify how to recruit, select, train, support, and retain operational staff. A systematic approach based on the integration of the human component will lead to enhanced system design, safety, efficiency, and operational performance. This project is part of the Human Technology Integration Thrust Area and Human Systems Research and Engineering Program within HFD.

Human Systems Engineering Research Project

Project Manager: Jennifer O'Connor, Ph.D.

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Science Division (HFD) projects examine human perception and ability to detect targets and threats as they pertain to the design of systems that maximize human performance, and the effectiveness of the technology operators use in the field. Results of this research allow the program to focus more closely on the psychological determiners that impact successful discrimination of threats and reduce false alarms. In addition to focusing on human perception, the project will also address how humans process information and how that impacts the human-machine interface. This project is part of the Human Technology Integration Thrust Area and Human Systems and Engineering Program within HFD.

Insider Threat Detection Program

Project Manager: Jennifer O'Connor, Ph.D.

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Insider Threat Detection Project will detect insider behavior that is likely to present or lead to a threat to critical infrastructure using behavioral indicators. Department of Homeland Security will collaborate with other U.S. agencies and international partners to move beyond the current focus on responses to accomplished hostile insider acts, and begin developing a greater capacity to deter and detect insider threats before substantial harm has been done. The immediate operational goal is to produce new and better tools to identify behavior patterns and characteristics identifiable before, during, and after employment that are associated with insider threats. This project is part of the Social and Behavioral Threat Analysis Thrust Area and Suspicious Behavior Detection Program withinHFD.

Mobile Biometrics System Project

Project Manager: Patty Wolfhope

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavior Sciences Division (HFD) Mobile Biometrics Project develops prototype technologies for mobile biometrics screening at remote sites along U.S. borders, during disasters and terrorist incidents, at sea, and in other places where communications access is limited. The goal is to demonstrate mobile biometrics screening capabilities and technologies that meet the future needs of Department operational users, but currently are not available with conventional biometrics systems. This project is part of the Personal Identification Systems Thrust Area and Biometrics Program within HFD.

Multi-modal Biometrics Project

Project Manager: Arun Vemury

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavior Sciences Division (HFD) Multi-modal Biometrics Project develops biometric technologies that accurately and rapidly identify individuals. The operational goal is to provide the capability to non-intrusively collect two or more biometrics (fingerprint, face image, and iris recognition) in less than ten seconds at a ninety-five percent acquisition rate without impeding the movement of individuals. The multi-modal technology will allow the Department to compare and match biometric samples from different sources, collected with different sensor technologies, under varying environmental conditions -- a capability that eludes existing technology. This project is part of the Personal Identification Systems Thrust Area and Biometrics Program within HFD.

Muslim Community Integration Project

Project Manager: Allison Smith, Ph.D.

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Muslim Community Integration Project conducts ethnographic research to examine the experiences of Muslims and non-Muslims in several communities throughout the U.S. The project will provide insights into the current state of Muslim communities focusing on their role and status in America and their perceptions of American society. This project is part of the Social and Behavioral Threat Analysis Thrust Area and Community Preparedness, Response and Recovery Program within HFD.

Predictive Screening Project

Project Manager: Larry Willis

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Counter-Improvised Explosives Devices (Counter-IED) Predictive Screening Project will derive observable behaviors that precede a suicide bombing attack and develop extraction algorithms to identify and alert personnel to indicators of suicide bombing behavior. HFD is executing this project as part of the Counter-IED Thrust Area and Predict Program.

Risk Prediction Project

Project Manager: Larry Willis

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Counter-Improvised Explosives Devices Risk Prediction Project will develop high speed software to identify improvised explosive device (IED) target and staging areas based upon group-and-cultural-specific tactics, techniques, and procedures derived from past foreign attacks. The goal is to use this information to prioritize the risk of likely potential targets of IED attacks within the United States. HFD is executing this project as part of the Counter-IED Thrust Area and Predict Program.

Social Network Analysis for Community Resilence Project

Project Manager: Michael Dunaway

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Social Network Analysis for Community Resilience Project develops a modeling capability for identifying formal and informal social networks that may be useful in enhancing preparedness and community resilience to natural disasters and terrorist events. This effort will leverage social network analysis research for understanding terrorist networks, social and financial transactions, and the spread of infectious diseases, and apply that knowledge to the construction of networks dedicated to strengthening local response capabilities and preparedness. It will also leverage past and on-going work from the Department of Defense (DOD) and other agencies. This project is part of the Social and Behavioral Threat Analysis Thrust Area and Community Preparedness and Resilience Program within HFD.

Violent Intent Modeling and Simulation Project

Project Manager: Ji Sun Lee

Project Overview: The Science and Technology (S&T) Directorate Human Factors/Behavioral Sciences Division (HFD) Violent Intent Modeling and Simulation Project develops intelligence analysis frameworks, including extraction of terrorist intention signatures, systematic estimation of future terrorist behavior based on social and behavioral sciences, and modeling and simulations of future terrorist behavior influences. It identifies leading edge social science modeling and simulation technologies and advances social science modeling and data fusion capabilities in such areas as hybrids of neural nets, structural equations, genetic algorithms, social networks, etc. This project is part of the Social and Behavioral Threat Analysis Thrust Area and Motivation and Intent Program within HFD.

Source: http://www.dhs.gov/files/programs/gc_1218480185439.shtm