AVIATION SECURITY RESEARCH AND DEVELOPMENT AT THE DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

COMMITTEE ON SCIENCE AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

APRIL 24, 2008

Serial No. 110–97

Printed for the use of the Committee on Science and Technology

Available via the World Wide Web: http://www.science.house.gov

U.S. GOVERNMENT PRINTING OFFICE

41–800PS WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SCIENCE AND TECHNOLOGY

HON. BART GORDON, Tennessee, *Chairman*

JERRY F. COSTELLO, Illinois	RALPH M. HALL, Texas
EDDIE BERNICE JOHNSON, Texas	F. JAMES SENSENBRENNER JR., Wisconsin
LYNN C. WOOLSEY, California	LAMAR S. SMITH, Texas
MARK UDALL, Colorado	DANA ROHRABACHER, California
DAVID WU, Oregon	ROSCOE G. BARTLETT, Maryland
BRIAN BAIRD, Washington	VERNON J. EHLERS, Michigan
BRAD MILLER, North Carolina	FRANK D. LUCAS, Oklahoma
DANIEL LIPINSKI, Illinois	JUDY BIGGERT, Illinois
NICK LAMPSON, Texas	W. TODD AKIN, Missouri
GABRIELLE GIFFORDS, Arizona	JO BONNER, Alabama
JERRY MCNERNEY, California	TOM FEENEY, Florida
LAURA RICHARDSON, California	RANDY NEUGEBAUER, Texas
PAUL KANJORSKI, Pennsylvania	BOB INGLIS, South Carolina
DARLENE HOOLEY, Oregon	DAVID G. REICHERT, Washington
STEVEN R. ROTHMAN, New Jersey	MICHAEL T. MCCAUL, Texas
JIM MATHESON, Utah	MARIO DIAZ-BALART, Florida
MIKE ROSS, Arkansas	PHIL GINGREY, Georgia
BEN CHANDLER, Kentucky	BRIAN P. BILBRAY, California
RUSS CARNAHAN, Missouri	ADRIAN SMITH, Nebraska
CHARLIE MELANCON, Louisiana	PAUL C. BROUN, Georgia
BARON P. HILL, Indiana	
HARRY E. MITCHELL, Arizona	
CHARLES A. WILSON, Ohio	

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. DAVID WU, Oregon, *Chairman*

JIM MATHESON, Utah	PHIL GINGREY, Georgia
HARRY E. MITCHELL, Arizona	VERNON J. EHLERS, Michigan
CHARLIE A. WILSON, Ohio	JUDY BIGGERT, Illinois
BEN CHANDLER, Kentucky	ADRIAN SMITH, Nebraska
MIKE ROSS, Arizona	PAUL C. BROUN, Georgia
LAURA RICHARDSON, California	
BART GORDON, Tennessee	RALPH M. HALL, Texas

MIKE QUEAR *Subcommittee Staff Director*
RACHEL JAGODA BRUNETTE *Democratic Professional Staff Member*
MEGHAN HOUSEWRIGHT *Democratic Professional Staff Member*
TIND SHEPPER RYEN *Republican Professional Staff Member*
PIPER LARGENT *Republican Professional Staff Member*

CONTENTS

April 24, 2008

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative David Wu, Chairman, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	6
Written Statement	7
Statement by Representative Phil Gingrey, Ranking Minority Member, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	7
Written Statement	9
Prepared Statement by Representative Laura Richardson, Member, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	9
Prepared Statement by Representative Harry E. Mitchell, Member, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	10
Prepared Statement by Representative Adrian Smith, Member, Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives	10

Witnesses:

Dr. Susan Hallowell, Director, Transportation Security Laboratory, Science and Technology Directorate, Department of Homeland Security	
Oral Statement	11
Written Statement	13
Biography	19
Mr. Adam Tsao, Chief of Staff, Office of Operational Process and Technology, Transportation Security Administration, Department of Homeland Security	
Oral Statement	20
Written Statement	21
Dr. Jimmie C. Oxley, Professor of Chemistry, University of Rhode Island (URI); Co-Director, URI Forensic Science Partnership; Co-Director, DHS University Center of Excellence in Explosive Detection, Mitigation, and Response	
Oral Statement	23
Written Statement	24
Biography	27
Dr. Colin G. Drury, Distinguished Professor and Chair, Department of Industrial and Systems Engineering, State University of New York at Buffalo	
Oral Statement	27
Written Statement	29
Biography	32
Discussion	34

Page

Appendix: Answers to Post-Hearing Questions

Dr. Susan Hallowell, Director, Transportation Security Laboratory, Science and Technology Directorate, Department of Homeland Security 44
Mr. Adam Tsao, Chief of Staff, Office of Operational Process and Technology, Transportation Security Administration, Department of Homeland Security 51
Dr. Jimmie C. Oxley, Professor of Chemistry, University of Rhode Island (URI); Co-Director, URI Forensic Science Partnership; Co-Director, DHS University Center of Excellence in Explosive Detection, Mitigation, and Response 55
Dr. Colin G. Drury, Distinguished Professor and Chair, Department of Industrial and Systems Engineering, State University of New York at Buffalo 56

AVIATION SECURITY RESEARCH AND DEVELOPMENT AT THE DEPARTMENT OF HOMELAND SECURITY

THURSDAY, APRIL 24, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, DC.

The Subcommittee met, pursuant to call, at 1:10 p.m., in Room 2318 of the Rayburn House Office Building, Hon. David Wu [Chairman of the Subcommittee] presiding.

BART GORDON, TENNESSEE
CHAIRMAN

RALPH M. HALL, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE AND TECHNOLOGY

SUITE 2320 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6375
TTY: (202) 226–4410
http://science.house.gov

The Subcommittee on Technology and Innovation

Hearing on:

Aviation Security Research and Development at the Department of Homeland Security

Thursday, April 24, 2008
1:00 p.m. – 3:00 p.m.
2318 Rayburn House Office Building

WITNESS LIST

Dr. Susan Hallowell
Director, Transportation Security Laboratory
Department of Homeland Security

Mr. Adam Tsao
Chief of Staff, Office of Operational Process and Technology
Transportation Security Administration
Department of Homeland Security

Dr. Jimmie Oxley
Professor of Chemistry
University of Rhode Island
Co-Director
DHS Center of Excellence for Explosives Detection, Mitigation, and Response

Dr. Colin Drury
Distinguished professor and Chair
Department of Industrial Engineering
University at Buffalo
State University of New York

HEARING CHARTER

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION
COMMITTEE ON SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

Aviation Security Research and Development at the Department of Homeland Security

THURSDAY, APRIL 24, 2008
1:00 P.M.–3:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

1. Purpose

On Thursday, April 24, 2008, the Subcommittee on Technology and Innovation will hold a hearing to review the aviation security-related research, development, testing, and evaluation (RDT&E) activities of the Department of Homeland Security (DHS). This hearing will also explore how the Transportation Security Laboratory and other components of DHS support the needs of the Transportation Security Administration, the aviation industry, and passengers generally through research, development, and education.

2. Witnesses

Dr. Susan Hallowell is the Director of the Transportation Security Laboratory (TSL), a component of the Department of Homeland Security's Science and Technology Directorate (DHS S&T).

Mr. Adam Tsao is the Chief of Staff of the Office of Operational Process and Technology of the Transportation Security Administration (TSA).

Dr. Jimmie Oxley is a Professor of Chemistry at the University of Rhode Island and Co-Director of the DHS Center of Excellence for Explosives Detection, Mitigation, and Response.

Dr. Colin Drury is a distinguished Professor and Chair of the Department of Industrial Engineering at the University at Buffalo.

3. Brief Overview

- The Transportation Security Administration (TSA) was created in 2001 to act as a centralized federal authority to manage transportation security efforts in the United States. The Transportation Security Laboratory (TSL) provides support for TSA's mission through research, technology development, testing and evaluation, and technical support for deployed technologies. TSL became part of the Department of Homeland Security Science and Technology Directorate in FY 2006. Previously, TSL was managed by the Federal Aviation Administration.
- Research priorities at TSL are generally set through the transportation security Integrated Product Team, which convenes stakeholder components of DHS, including TSA, to discuss capability gaps and determine which R&D projects are most likely to meet users' needs. Additionally, TSL coordinates with DHS S&T's explosives division and will work with the newly formed Center of Excellence for Explosives Detection, Mitigation, and Response. The lab also tests and certifies equipment submitted by outside vendors for eventual inclusion on TSA's qualified product list (QPL), which allows vendors to sell those products to TSA.
- Technology development priorities are also influenced by outside requirements stemming from intelligence or publicity of particular threats, such as the liquid explosives incident in August 2006.
- TSL has particular expertise in testing and evaluation, and hosts specialized laboratories capable of handling explosives for technology validation. However, TSL currently does not have the capacity to test screening technologies

in a realistic setting, where a network of devices are used to detect potential threats. Additionally, TSL does not carry out field tests of technology, but does provide technical support to TSA for technologies in use at airports.

4. Issues and Concerns

Will the ongoing research, development, testing and evaluation projects at the Transportation Security Laboratory (TSL) meet the Transportation Security Administration's present and future needs? Is there adequate investment in basic research at TSL to allow the lab enough flexibility to address rapidly emerging threats? TSA is responsible for setting technology development priorities at TSL through the Integrated Product Team process, but budget limitations and demand for immediate technological responses to high-profile threats (such as liquid explosives or shoe bombs) can distract the lab from longer-term needs. Additionally, because of variations in airport design and passenger capacity, TSA cannot have a standard checkpoint design that works at every airport. A good solution to these conflicting pressures is strong investment in basic research, which provides the scientific basis to allow the laboratory to be flexible in its response to emerging threats and varying needs.

Does TSL's testing and evaluation of aviation security technology provide adequate information to the end-users at TSA? How are the tests designed, and what are the criteria for success? Are technologies that are tested or certified by TSL ready for deployment? If not, what additional efforts are necessary to bring technologies to full readiness, and how does TSL contribute to those efforts? TSL's testing and evaluation (T&E) protocols are considered a model for the Department of Homeland Security, but some technologies are deployed by TSA in spite of technical or operational issues (TSL does not control deployment schedules). Many of these issues could be identified or resolved if TSL was able to test devices in a realistic checkpoint scenario that incorporates a networked system of devices and carries out tests based on screeners' and passengers' needs and capabilities. Moreover, as technology develops, TSL must continually update performance and technical standards to address new capabilities and new requirements.

Additionally, at its current capacity, TSL will likely have an increasingly difficult time keeping up with TSA's needs. According to the Director of TSL, their work for TSA has tripled since April 2006 while funding for the lab has decreased. If this imbalance continues, T&E capabilities at TSL will continue to suffer.

Does TSL adequately incorporate human factors engineering and human-technology interface principles into technology design and testing? How do TSA and TSL test and evaluate whether human-technology interface principles have been properly applied in the design and manufacturing of aviation security technologies? To move passengers and luggage efficiently through checkpoints, screeners need technology to help them search for contraband or dangerous items. As the list of forbidden items grows in response to newly identified threats, screeners' jobs become more and more difficult and need improved technological responses. The best technologies take into account screeners' technical skills and needs and looks at the "human-technology interface;" how well technology meshes with those skills and needs. Moreover, since these technologies are used in a public setting, passenger acceptance is also crucial. Designers must consider whether passengers would object or be seriously inconvenienced by technologies before they are deployed to avoid public outcry that might ultimately harm the aviation industry by driving away customers. Some recent controversies, such as the deployment of the back-scatter machine—which appears to virtually strip-search passengers-could have been avoided through careful attention to human-technology interface issues.

5. Background

Technology plays a major role in aviation security operations. Screeners employed by the Transportation Security Administration (TSA) employ a variety of sensors to scan passengers and luggage for dangerous items quickly and efficiently. Many of these technologies, as well as other security devices, are developed, tested, or certified at the Transportation Security Laboratory (TSL) in Atlantic City, NJ. This lab, part of the DHS S&T Directorate, conducts research, development, testing, and evaluation (RDT&E) for explosives detection and other transportation security related technologies with the goal of deploying these technologies to TSA.

The Transportation Security Laboratory, a component of the Federal Aviation Administration (FAA) and TSA before its transfer to the DHS Science and Technology

Directorate in FY 2006, hosts specialized facilities for research, development, testing, and evaluation of innovative technologies for detecting threats to the transportation sector. In addition to basic and applied research and technology development, TSL carries out certification, qualification, and assessments of technologies developed by private industry for use by TSA.

The laboratory has built capacity in a number of technology areas critical to transportation security, including bulk and trace sensors, devices for understanding the physics of explosions, technology for enhancing explosion survivability, communications equipment, and access control technologies. There are also six laboratories at TSL dedicated to testing explosives and weapons detection equipment. Finally, in addition to its RDT&E capacity, TSL also maintains models of all deployed technologies at the Atlantic City facility for troubleshooting and technical support purposes.

RDT&E priorities for TSL are generally set by TSA, though they are influenced by the work of other DHS S&T components, including the Homeland Security Science and Technology Advisory Committee (HSSTAC) and the DHS S&T Explosives Division. DHS S&T uses a formal process that convenes Integrated Product Teams (IPTs) comprised of officials from DHS components who advise the S&T Directorate on their technology needs, thus informing specific research priorities. The planned transportation security IPT will be lead by TSA and will include stakeholders such as U.S. Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE) and the U.S. Coast Guard (USCG) who will select transportation security related technology development projects for TSL to undertake. To date, TSA has indicated that they are especially interested in projects for enhancing checkpoint security. TSL also coordinates with the Explosives Division of DHS S&T, which is guided by a separate but related explosives IPT that is currently focusing on standoff detection of improvised explosive devices (IEDs).

TSA is also responsible for guiding testing and evaluation (T&E) priorities at TSL. Tests are constrained by the various lab capabilities, but TSL is able to carry out testing and validation for a wide array of technologies, including devices for baggage and personnel inspection, cargo inspection, infrastructure protection, and conveyance protection. The technologies that are tested at TSL include those developed internally, as well as by outside industry. TSA can specifically request certification of outside products for a qualified product list (QPL) that TSA uses to determine whether a technology is suitable for procurement and deployment. The laboratory will also begin developing plans to create a testing facility to model a full airport checkpoint, which would examine the technical performance of various technologies when they are integrated into a realistic system. TSA is also planning to build a similar facility for field testing technologies that are integrated into a checkpoint, but the aim of that facility would be technology operations and robustness.

Chairman WU. I would like to welcome everyone to this afternoon's hearing on aviation security research and development at the Department of Homeland Security. Since 2001, aviation security has vastly improved. There are new policies in place to help protect passengers and aircraft, and aviation security professionals are better trained to detect dangerous items. Of course, technology plays a critical role. Significant advances in aviation security technologies have led to screening equipment that is faster and more reliable than the last generation, allowing Transportation Security Administration screeners to process passengers and baggage efficiently while still keeping prohibited items off planes.

However, improvements still need to be made. Last year, a Government Accountability Office test of airport checkpoints found that explosive devices could be smuggled through undetected. There have also been recent news reports highlighting security failures, including a January 2008 CNN segment that featured a TSA employee slipping a bomb past screeners in a planned test. One of GAO's key recommendations for dealing with these shortcomings was to invest in improving security technologies.

The Transportation Security Laboratory, or TSL, is at the forefront of developing the next generation of aviation security technology. This laboratory, which was transferred to the DHS Science and Technology Directorate in fiscal year 2006, serves as the Nation's key resource for transportation security-related research, development, testing, and evaluation. In addition to groundbreaking research on explosives, TSL develops and validates passenger and luggage screening technologies, certifies devices developed by private industry, and provides technical support to TSA for deployed technologies.

Rigorous testing and evaluation are an important step towards ensuring that new technologies meet TSA's technical needs. Currently, TSA works closely with the laboratory to develop test protocols and define criteria for success. But the security failures discovered by GAO and others illustrate the need to constantly update tests to ensure that technologies can deal with emerging threats. Technologies deployed before they are truly ready cement the perception that aviation security is nothing but theater.

Finally, we often forget that a technology is only as successful as the person operating it, and this is especially true in the aviation security sector, where screeners must determine whether objects identified by screening technologies are truly dangerous. Additionally, passengers also play a key role in any technology's performance and success. If passengers find screening technologies too cumbersome or too intrusive, the consequences can ripple across the entire aviation sector. TSL and TSA must work together to ensure that human factors are taken into consideration from the first stages of technologic development.

Dr. Hallowell has said in the past that she envisions a checkpoint in the future where no one has to empty their pockets, take off their shoes, or try to fit their toothpaste and deodorant into a tiny plastic bag in order to get on an airplane, and I for one truly look forward to that day. The Committee applauds that goal, and I want to work with you all and the TSA to ensure that the next generation aviation security technologies are effective and efficient while meeting the needs of all screeners and passengers.

I would now like to recognize my friend and colleague, the Ranking Member from Georgia, Dr. Gingrey, for his opening statement.

[The prepared statement of Chairman Wu follows:]

PREPARED STATEMENT OF CHAIRMAN DAVID WU

This hearing will come to order. Good afternoon. I'd like to welcome everyone to this afternoon's hearing on *Aviation Security Research and Development at the Department of Homeland Security.*

Since 2001, aviation security has vastly improved. There are new policies in place to help protect passengers and aircraft, and aviation security professionals are better trained to detect dangerous items. Of course, technology plays a critical role. Significant advances in aviation security technologies have led to screening equipment that is faster and more reliable than the last generation, allowing Transportation Security Administration screeners to process passengers and baggage efficiently while still keeping prohibited items off planes.

However, improvements still need to be made.

Last year, a Government Accountability Office test of airport checkpoints found that explosive devices could be smuggled through undetected. There have also been recent news reports highlighting security failures, including a January 2008 CNN segment that featured a TSA employee slipping a bomb past screeners in a planned test. One of GAO's key recommendations for dealing with these shortcomings was to invest in improving security technologies.

The Transportation Security Laboratory, or TSL, is at the forefront of developing the next generation of aviation security technology. This laboratory, which was transferred to the DHS Science and Technology Directorate in FY 2006, serves as the Nation's key resource for transportation security-related research, development, testing, and evaluation. In addition to ground-breaking research on explosives, TSL develops and validates passenger and luggage screening technologies, certifies devices developed by private industry, and provides critical technical support to TSA for deployed technologies.

Rigorous testing and evaluation are a crucial step towards ensuring that new technologies meet TSA's technical needs. Currently, TSA works closely with the laboratory to develop test protocols and define criteria for success. But the security failures discovered by GAO and others illustrate the need to constantly update tests to ensure that technologies can deal with emerging threats. Technologies deployed before they are truly ready cement the perception that aviation security is nothing but theater.

Finally, we often forget that a technology is only as successful as the person operating it. This is especially true in the aviation security sector, where screeners must determine whether objects identified by screening technologies are truly dangerous. Additionally, passengers also play a key role in any technology's performance and success. If passengers find screening technologies too cumbersome or too intrusive, the consequences can ripple across the entire aviation sector. TSL and TSA must work together to ensure that human factors are taken into consideration from the first stages of technology development.

Dr. Hallowell has said in the past that she envisions a checkpoint of the future where no one has to empty their pockets, take off their shoes, or try to fit their toothpaste and deodorant into a tiny plastic bag in order to get on an airplane. The Committee applauds that goal, and I want to work with you and the TSA to ensure that next generation aviation security technologies are effective and efficient while meeting the needs of all screeners and passengers.

I'd now like to recognize my colleague, the Ranking Member from Georgia, Dr. Gingrey, for an opening statement.

Mr. GINGREY. Good afternoon, Chairman Wu, and I want to apologize in advance to our distinguished panel because I am going to have to step out after I make the opening statement, hopefully to come back because I don't want to miss all of this important, very, very important hearing from such a distinguished panel. Dr. Oxley, I see you are a Professor of Chemistry. I have a degree, a BS, in chemistry from Georgia Tech from a long time ago. I hope if you are still doing any teaching that you grade a little easier than those monsters that I had at Georgia Tech. In any regard, Mr. Chairman, thank you for holding this important hearing today on the Department of Homeland Security's aviation security program.

Aviation security is an issue that affects every Member of Congress, as passengers across the country put their faith in the Transportation Security Administration to have the technology in place to keep them safe as they travel. We have an excellent opportunity today to discuss how to best put the immense creative talent of our country's scientists an engineers to use to prevent acts of terrorism in our airports and skies. Aviation continues to be a target, no question about it, as evidenced by the publicized liquid explosive plot from 2006 and of course the attempted attack by the famous, infamous shoe bomber, Richard Reid, back in 2001.

A successful attack like the tragic one that did occur on September 11, 2001, would yield an immediate and catastrophic loss of life, create economic losses throughout the aviation industry and possibly beyond. In fact, I think if that occurred today, it would be a lot more devastating economically than it was back in 2001, what with the price of jet fuel and the airlines struggling.

But there is no easy, all-encompassing solution against a cunning and committed enemy. We must continually review and refine every defense and seek out new ideas and technologies that will better nullify the threats that will continue to be there. And we must also recall that this is but one challenge to implementing an effective, efficient, and evolving defense of our homeland.

I am eager to hear what the witnesses have to say about this challenge and how we can improve our current aviation security efforts. Mr. Chairman, we must also ensure that our substantial investments of R&D and new aviation security technologies work as advertised. They are coordinated throughout the government, include appropriate university researchers and private-sector companies. And to that end, I am particularly interested in hearing how the TSA and Transportation Security Lab witnesses describe their relationship and what is the plan for the future. Formerly part of TSA, the Transportation Security Lab became part of the Science and Technology Directorate of the Department of Homeland Security back in 2006. The lab possesses many of the world's foremost experts on all kinds of aviation security technology and of course supports research, development, tests, and evaluation of activities based on the requirements and the priorities of TSA.

Within the wide aviation security industry, some have had difficulty understanding the roles and the responsibilities of TSA and TSL and how other institutions, like universities, national labs, or private companies can best contribute. I hope that our witnesses today will be able to clarify and clearly and concisely lay out who is developing our aviation security strategy and how that strategy is being implemented. How can a university researcher determine what TSA's most pressing, basic research needs are? How can a private company translate broad equipment requirements to technical specs that can lead to a commercially available product? Is there a standard process for tests and evaluation of new technologies? The answers to these questions will lessen confusion outside of the Department of Homeland Security and it will allow TSA to create more successful partnerships.

Again, Mr. Chairman, I look forward to hearing from our distinguished panel, and with that, I will yield back the balance of my time.

[The prepared statement of Mr. Gingrey follows:]

PREPARED STATEMENT OF REPRESENTATIVE PHIL GINGREY

Good afternoon, Chairman Wu. Thank you for holding this important hearing today on the Department of Homeland Security's aviation security programs. Aviation security is an issue that affects every Member of Congress as passengers across the country put their faith in the Transportation Security Administration to have the technology in place to keep them safe as they travel.

We have an excellent opportunity today to discuss how best to put the immense creative talent of our country's scientists and engineers to use to prevent acts of terrorism in our airports and skies.

Aviation continues to be a target, as evidenced by the publicized liquid explosives plot from 2006 and the attempted attack by "shoe bomber" Richard Reid in 2001. A successful attack like the tragic one that occurred on September 11, 2001 would yield an immediate and catastrophic loss of life, and create economic losses throughout the aviation industry and possibly beyond.

But there is no easy, all-encompassing solution. Against a guileful and committed enemy, we must continually review and refine our defenses and seek out new ideas and technologies that will better nullify the threats against us. We must also recall that this is but one challenge to implementing an effective, efficient, and evolving defense of our homeland. I am eager to hear what the witnesses have to say about this challenge and how we can improve our current aviation security efforts.

Mr. Chairman, we must also ensure that our substantial investments in R&D and new aviation security technologies work as advertised, are coordinated throughout the government, and include appropriate university researchers and private sector companies. To that end, I am particularly interested in hearing our TSA and Transportation Security Lab (TSL) witnesses describe their relationship and plans for the future.

Formerly part of TSA, the Transportation Security Lab became part of the Science and Technology Directorate of DHS in 2006. The lab possesses many of the world's foremost experts on all kinds of aviation security technology and supports research, development, test, and evaluation activities based on the requirements and priorities of TSA.

Within the wider aviation security industry, some have had difficulty understanding the roles and responsibilities of TSA and TSL and how other institutions like universities, national labs, or private companies can best contribute. I hope that our witnesses today will be able to clearly and concisely lay out who is developing our aviation security strategy and how that strategy is being implemented.

How can a university researcher determine what TSA's most pressing basic research needs are? How can a private company translate broad equipment requirements to technical specifications that can lead to a commercially available product?

Is there a standard process for test and evaluation of new technologies? Answers to these questions will lessen confusion outside of DHS and allow TSA to create more successful partnerships.

Again, I look forward to hearing from our distinguished panel and with that Mr. Chairman, I yield back the balance of my time.

Chairman WU. Thank you, Dr. Gingrey, and we look forward to your return once you have taken care of other very important tasks.

If there are other Members who wish to submit additional opening statements, the statements will be added at this point in the record.

[The prepared statement of Ms. Richardson follows:]

PREPARED STATEMENT OF REPRESENTATIVE LAURA RICHARDSON

Thank you Chairman Wu for holding this very important hearing today, and our witnesses for your attendance.

In a post 9/11 world, is there a topic that is more important than the one we are discussing today? That awful day back in 2001 stole our innocence and put our nation and Congress on high alert. No longer could we take for granted the safety of the two million passengers that pass through our nations airports. Our enemies raised the stakes, and it was critical that we responded thoroughly in order to minimize the chances that an event like 9/11 could never happen again.

While there has not been another terrorist attack on our soil since 9/11, at times it seems like we are two steps behind the terrorist in a reactionary mode. First there was the shoe bomb incident. As a result we all have to take our shoes off when we pass through security checkpoints. Then there was the threat of liquid explosives, which forced TSA to ban passengers from carrying liquids on board. While no one could have predicted these events, it is imperative that TSA and other federal agencies tasked with protecting all of us are more proactive in their attempts to protect us. This can be achieved if we were to heed the advice that our witness Jimmie C. Oxley offered in his written testimony, and that is to "increase communication to technology suppliers with respect to emerging threats, scenarios and threat levels." We simply can not protect ourselves, if our researchers do not know the extent of the threat.

On that note my staff recently had the opportunity to visit the National Institute of Standards and Technology (NIST) laboratories in Gaithersburg, MD, where the scientist there are conducting research into trace explosive detection. While the Transportation Security Laboratory (TSL) is the primary source for aviation security R&D, I hope that these two agencies can collaborate on more research projects, because every federal agency plays a vital role in aviation security on some level.

Let me conclude by stating that the timing of this hearing could not be better as most of my colleagues, including myself will travel by air back to our districts for the weekend.

I look forward to this discussion, and I hope that we as a committee can learn from this hearing what we can do to assist TSA, and DSH in their ongoing efforts to protect all who travel in the United States.

Mr. Chairman I yield back my time.

[The prepared statement of Mr. Mitchell follows:]

PREPARED STATEMENT OF REPRESENTATIVE HARRY E. MITCHELL

Thank you, Mr. Chairman.

The Transportation Security Administration (TSA) is tasked with managing transportation security efforts to ensure that our airline passengers can fly safely.

However, as the number and type of threats continues to increase, it is essential to ensure that TSA has the tools it needs to protect airline passengers.

The Transportation Security Laboratory (TSL) supports the TSA through research, technology development, testing and evaluation, and testing support for security technologies.

Clearly safety and security must be our top priorities. But we also need to ensure that our new technologies are practical, and can work in a realistic passenger screening setting.

I look forward to hearing more from our witness on how we can keep our passengers safe.

I yield back.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF REPRESENTATIVE ADRIAN SMITH

Thank you Chairman Wu. It's a pleasure to be here this afternoon for this subcommittee hearing on the Department of Homeland Security's Transportation Security Laboratory and aviation security. Subcommittee Ranking Member Gingrey has been detained at a meeting of the House Armed Services Committee and will be joining this hearing when possible. He has an insightful opening statement that he will submit for the record and which I urge everyone to read.

There is an obvious and immediate need for improvements in aviation security within the U.S. and around the world. Airlines continue to be targeted for attack, and new types of threats are being exposed everyday. We need the help and support of scientists and engineers to defend against the wide variety of explosives and weapons that could be used in an attack.

Members of Congress take a lot of flights back and forth between Washington and our homes. And while we may feel like aviation security experts ourselves after the hundredth flight, the real expertise is before us today. The panel has a wealth of experience and knowledge in this area, and I'm looking forward to learning what I can from you.

Before closing, I would also like to echo a statement in Dr. Gingrey's prepared remarks. A large number of companies and individual researchers have looked at how they might improve aviation security after the tragic events of 9–11. However, within this wider aviation security industry, the roles and responsibilities of TSA, TSL, and other institutions like universities, national labs, or private companies are poorly understood. In your testimony today, I hope the witnesses can provide clear and concise guidance for how our aviation security strategy is set and how that strategy impacts technology development.

Again, thank you for taking the time to speak with us today. Mr. Chairman, I will yield back the balance of my time.

Chairman WU. And now I am delighted to introduce our expert panel. Dr. Susan Hallowell is the Director of the Transportation Security Laboratory. Mr. Adam Tsao is the Chief of Staff of the Office of Operational Process and Technology which handles technology procurement issues for the Transportation Security Administration. I actually had to read that phrase three times this morning so I wouldn't trip over it right now. Dr. Jimmie Oxley is a Professor of Chemistry at the University of Rhode Island and is the Co-Director of the newly awarded DHS University Center of Excellence for Explosives Detection—see, I should have read that more carefully—Explosives Detection, Mitigation, and Response. And finally, Dr. Colin Drury is a Distinguished Professor and Chair of the Department of Industrial Engineering at the State University of New York at Buffalo.

As our witnesses should know, spoken testimony should be about five minutes long after which the Members of the Committee will have five minutes each to ask questions. Please feel free to summarize your written testimony, and we shall begin with Dr. Hallowell.

STATEMENT OF DR. SUSAN HALLOWELL, DIRECTOR, TRANSPORTATION SECURITY LABORATORY, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Dr. HALLOWELL. Good afternoon, Chairman Wu and distinguished Members of the Committee. It is an honor for me to appear before you today and provide information about the Transportation Security Laboratory which is part of the Department of Homeland Security's Science and Technology Directorate.

The Transportation Security Laboratory has historically been responsible for turning aviation security applied research into prototypes and products. Following the PanAm 103 tragedy in 1988, the Aviation Security Improvement Act was enacted by Congress. This law mandated the development of technology that could be certified to be reliable and detect explosive materials concealed in checked baggage. This resulted in the creation of the Aviation Security Laboratory, my lab, which at that time was an element of the Federal Aviation Administration in 1992.

The ASL received direct funding by congressional line explosives detection, infrastructure protection, human factors, and aircraft hardening. Congress also required that the FAA develop a certification standard that would define the performance requirements for an explosive detection system which we call EDS in terms of probability of detection, false alarm rates, throughput rates, and detection of specific types and configurations of different kinds of explosives. The EDS Certification Standard was established and published in the Federal Register in 1992, and the lab certified its first EDS unit in 1994.

The ASL was integrated into the newly formed TSA after the terrorist attacks on 9/11 and was renamed the Transportation Security Laboratory. The TSL provided the intensive accelerated effort necessary to develop, mature, and certify technologies necessary to support the historic deployment of aviation security technology screening devices in American airports. During this timeframe, new standards of performance were created for TSA and several technologies were qualified or certified. In 2003, the TSA and the TSL joined the new Department of Homeland Security; and in 2006, the TSL became part of the Department's Science and Technology Directorate.

In the ever-changing landscape of potential threats, the Transportation Security Lab continues to be recognized as the foremost resource for applied research development, integration, and validation of leading-edge science and technology for detection and mitigation of explosives and conventional threats.

The lab continues to work to provide both technical and procedural solutions that will work in the field. The TSL performs R&D at the request of the S&T directorate. The laboratory currently supports S&T explosives division, checked baggage, air cargo, and checkpoint program efforts. TSL also performs work for the TSA on an as-required basis. This includes certification, qualification tests, and technology assessment testing. TSL is also the go-to laboratory for a number of government agencies that are looking for explosive detection devices.

Tests and evaluation activities at the TSL encompass two independent functions. The independent tests and evaluation function is responsible for evaluating mature technologies that may meet TSA security requirements that are suitable for piloting or deployment, and principally this supports the TSA needs. The research, development, test, and evaluation function has responsibilities ranging from evaluation of applied research, to prototype development and maturation and supports S&T or other R&D customers that we have at the laboratory.

These two groups set their priorities using different methodologies. The IT&E group has a strong relationship with TSA's Office of Security Technology in that they frequently discuss testing requirements, priorities, and the results of those testing evaluations. Results support TSA decisions for field trials, deployment, or their investment strategies. The IT&E office judges detection worthiness and product readiness. The customer of TSA sets the requirements, and the laboratory designs each test to determine if candidate systems meet those requirements. The types and frequencies of independent testing at the TSL has tripled in the last two years as acquisition by TSA has become more diverse as more explosives and more weapons detection equipment has become commercially available for testing.

In general, there are three kinds of tests administered by the independent testing evaluation team. The Certification Test is focused on providing laboratory certification of matured explosive detection equipment. Certification is recognized as the world standard for explosives detection.

The Qualification Tests are designed to verify that a security system meets the requirements specified in the TSA-initiated Technical Requirements Document. The results from this test, along with TSA-conducted pilots, field trials, generally result in a determination of fitness-for-use by TSA.

Laboratory Assessment Testing is conducted to determine the general capability of a system. The results of these evaluations of candidate security systems drive future development efforts or operational evaluations.

DT&E testing at the TSL assesses the strengths, weaknesses, and the vulnerabilities of technologies as they mature. The primary focus is to ensure that technology is robust and ready to go to the final stages of testing done by the independent test and evaluation group.

While the TSL performs testing certification of technologies, its responsibility of TSA as our customer——

Chairman WU. Dr. Hallowell, if you wouldn't mind summing up in just a little bit.

Dr. HALLOWELL. Certainly, sir. In conclusion, I would just like to say that the focus of R&D and test evaluation is done by the TSL, and our focus is to develop immature and transitioning technology to detect explosives. We have a close relationship with our customer which is TSA, and it allows us to understand the customer needs. The TSL does stand proudly behind the fact that every piece of security equipment that is in American airports has gone through the hands of people in our laboratory.

Chairman Wu and Ranking Member who left and distinguished Members of the Committee, I want to thank you for giving me the opportunity to provide this testimony.

[The prepared statement of Dr. Hallowell follows:]

PREPARED STATEMENT OF SUSAN HALLOWELL

INTRODUCTION

Good Afternoon Chairman Wu, Ranking Member Gingrey, and distinguished Members of the Committee. It is an honor for me to appear before you today to provide you with information about the Transportation Security Laboratory, part of the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T).

The Transportation Security Laboratory (TSL) has historically been responsible for turning aviation security applied research into prototypes and products. The Laboratory emerged from many years of work by Federal Aviation Authority (FAA) officials to increase aviation security, originally in the light of high-jacking incidents in the 1970s. The *Air Transportation Security Act of 1974* (Public Law 93–366) granted the FAA authority to pursue methods aimed at preventing high-jacking, and this authority was strengthened by the 1985 *International Security and Development Cooperation Act* (Public Law 99–83), which led to growth and expansion of the FAA's research and development program.

During the 1980s, threats to aviation safety began to include bombs as well as high-jacking threats, and the sorts of technology needed for detection and screening purposes started to change. Following the PanAm 103 tragedy in 1988, development of state-of-the-art technology that the FAA Administrator could certify as reliably able to detect explosive material in checked baggage was recommended. These recommendations, codified in the *Aviation Security Improvement Act* (Public Law 101–604) in 1992, resulted in the creation of the Aviation Security Laboratory (ASL) at the FAA William J. Hughes Technical Center, in Atlantic City, New Jersey.

The new ASL launched a multi-tiered program to develop automatic methods to detect threat amounts of explosive in checked luggage as well as develop hardened aircraft containers capable of preventing another tragedy. The ASL received direct funding by congressional line explosives detection, infrastructure protection, human factors, and aircraft hardening. The Commission's mandate also required that the FAA develop a Certification Standard that would define the performance requirements for an Explosive Detection System (EDS) in terms of probability of detection, false alarm rate, throughput rate, and detection of specific types and configuration of explosives. The EDS Certification Standard was established and published in the *Federal Register* in 1992, and the ASL certified the first unit, an InVision CTX 5000 System, in 1994.

Following the events of 9/11, the Aviation Security Laboratory was renamed the Transportation Security Laboratory (TSL) and joined the Transportation Security Administration (TSA); in 2003, the TSA and the TSL joined the new Department of Homeland Security, and in 2006 the TSL became part of the Department's Science and Technology Directorate. As a federal laboratory and extension of the Directorate, the TSL's domain and customer base continue to grow. In the dynamic environment in which we live, where both foreign and domestic entities pose real threats, the Transportation Security Laboratory is recognized as the foremost resource for applied research, development, integration, and validation of leading edge science and technology for the detection and mitigation of explosives and conventional weapons threats. The Laboratory is more than a research institution, however; it is committed to providing technical and procedural solutions that work in the field. This testimony provides an overview of TSL's research, development, test and evaluation activities, its customer interactions, and its roles in technology transfer.

TSL's Role in Setting Aviation Security Research, Development, Testing and Evaluation Priorities

Although the TSL provides research and development (R&D) input, the TSL does not set priorities for this work. The TSL performs R&D at the request of the S&T Directorate, and priorities for this work are set primarily by the customer components. Under Secretary Cohen instituted the Capstone Integrated Product Team (IPT) process to set priorities for the Transition portion of the S&T Directorate's budget. Transition programs are focused on providing technology solutions to meet customer need in the zero to three years timeframe. Through this process our customers identify and prioritize their capability gaps to mission performance, which allows the Directorate to respond with applicable technology solutions to fill these gaps. Aviation security efforts fall under the Transportation Security Capstone IPT managed by the S&T Directorate's Explosive Division. TSA is the customer lead for this IPT. TSL currently supports S&T Explosives Division's checked baggage, air cargo, and checkpoint program efforts. The Research portion of the Directorate's budget is not completely tied to Transition programs but aligned to provide breakthrough science to support longer-term (outside of three years) needs of the customer.

The Capstone process has lead to a better understanding of customer needs and how they set priorities, but it also has challenges given the large number of identified capability gaps and the expanded role of the Explosives Division beyond aviation and transportation explosives detection. As a result, the current funding for aviation security R&D for explosives detection is about what it was in 1996 (in absolute dollars).

With the use of S&T 'Core Funding' resources, TSL also performs work for customers on an as-requested basis. This involves pop-up requests from TSA, both from the TSA Office of Security Technology (OST), and from TSA field offices and airports. TSL has also done work for the U.S. Secret Service, the U.S. Coast Guard, DHS Customs and Border Protection, the Department of State, and the Department of Defense. These organizations utilize the TSL as a 'go-to' laboratory for explosives detection RDT&E. The lab conducts RDT&E evaluations of commercial off-the-shelf (COTS) and next-generation prototype detection equipment, provides laboratory and field testing standards for deployed explosives detection systems, and acts as subject matter experts to consult on a wide variety of issues involving weapons and explosives detection.

Test and evaluations activities at TSL encompass two independent functions: The Independent Test and Evaluation (IT&E) function is responsible for evaluating mature technology that may meet TSA's security requirements, suitable for piloting or deployment, and the Research and Development function has responsibilities ranging from applied research, to prototype development, to technology maturation that produces prototypes suitable for evaluation by the Independent Test and Evaluation Team. These two groups set their priorities using different methodologies.

The IT&E group has a strong relationship with the TSA's OST, in that they frequently discuss testing requirements, priorities and results of evaluations. TSL conducts three main kinds of independent verification and validation tests: certification tests, qualification tests, and laboratory assessments. These will be discussed in greater detail in the next section of my testimony, "TSL's Testing and Evaluation Procedures."

The types and frequency of independent testing at the TSL has tripled in the last two years, as acquisitions by TSA have become more diverse and more explosives and weapons detection equipment has become commercially available. The Department of Homeland Security Appropriations Bill for FY 2008 directs DHS S&T "to report on the costs and benefits of charging companies for certification of their products (at Transportation Security Laboratory (TSL)) in light of the potential to provide enhanced certification services and the capital improvement needed to safely house the ITE program." S&T has performed the review as directed and believes that TSL should be allowed to charge companies for certification of their products. Since 1992, the TSL has carried out their Congressional responsibilities while serving as the focal point for technical exchange and excellence in the field of security technology with industry, academia, other federal and State agencies and foreign governments. Allowing TSL to charge companies for certification of their products is appropriate for this enduring and mature laboratory. The scope of investment required to meet the expanding workload of the Lab addresses infrastructure and personnel investment required.

TSL's Testing and Evaluation Procedures

Review of test and evaluation activities. There are different kinds of Test and Evaluation (T&E) activities at the TSL. Independent Test and Evaluation Activities include certification, qualification, and assessment testing, and generally speaking, are performed to determine if detection systems meet customer defined requirements. Developmental Test and Evaluation Activities (DT&E) activities are designed to verify that a prototype or near COTS system has met performance metrics established within the R&D program, such that it can proceed to the next R&D stage. Additionally, R&D may look at the science and technology issues behind the technology, along with the development of critical simulants or standards to perform laboratory or field testing of explosives.

Independent Test & Evaluation: TSL's Independent Test and Evaluation (IT&E) group conducts independent verification and validation of detection systems for transportation commerce inspection (people, goods, and baggage). Results support decisions of DHS operating elements (such as TSA) for field trials and production or deployment, as well as key program milestones, bench-marking, and investment strategy. The IT&E office judges "detection-worthiness" and product readiness. The customer sets the requirements, and TSL designs each test to determine if candidate systems meet those requirements.

The *Certification Test* Program is reserved for detection testing of bulk and trace explosives detection systems and equipment under statutory authority 49 U.S.C. §44913 for checked baggage. The focus is on providing laboratory certification of matured explosives detection equipment, certifying that salient performance characteristics, such as the probability of detection of all categories of explosives with appropriate false alarm rates and throughput rates, are met. The details of types and masses of explosives and false alarm rates are classified. EDS must be certified before they can be deployed. P.L. 101–604 defined the requirement for certification of Explosives Detection Systems (EDS), and P.L. 107–71 defined the requirement for certification for Trace Explosives Detection Systems. Certification is recognized as a world standard for explosives detection. The TSL is ISO 9001:2000 registered for certification of explosive detection systems.

The certification process is clearly defined in the EDS Certification Management Plan (1993) which is available to those entities seeking systems certification. The certification test protocols were developed by a panel of experts (the National Academy of Sciences). Certification tests are performed with dedicated personnel, with the Test Director and an independent third party observer present. In the last two years, TSL has certified eleven bulk EDS and six trace EDS.

Qualification Tests are designed to verify that a security system meets customer-defined requirements as specified in a TSA-initiated Technical Requirements Document. This test, along with piloting (field trials) generally results in a determination of fitness-for-use. This process is modeled after the certification process, and is defined within the Qualification Management Plan. Unlike the Certification Test, the requirements of the Qualification Management Plan typically expand beyond detection functions to include operational requirements. The Qualification Test Program is conducted under statutory authority different from certification testing. Covered by 10 U.S.C. 2319, 41 U.S.C. 253(e) and FAR Subpart 9.2 Qualification Requirements, the result of Qualification Testing is a recommendation of whether candidate systems should be placed on a Qualified Products List (QPL). TSL has conducted 56 qualification tests in the last two years.

Laboratory Assessment Testing is conducted to determine the general capability of a system. These evaluations of candidate security systems are carried out in accordance with interim performance metrics, and the results drive future development efforts or operational deployment evaluations. While the IT&E group practices best scientific principles in test design, execution, and evaluation of data, assessment criteria are determined by the customer (TSA) and the customer's needs. TSL has conducted 124 such assessments in the last two years on bulk EDS and 26 on trace EDS in the last two years.

Developmental Test and Evaluation (DT&E) is performed by the R&D team at the TSL, and involves testing in a controlled environment to ensure that all system or product components meet technical specifications. These tests are designed to ensure that developmental products have met major milestones identified within the R&D project.

DT&E testing at the TSL assesses the strengths, weaknesses, and vulnerabilities of technologies as they mature and gain capability. The primary focus is to ensure that the technology is robust and ready for Certification Testing. The criteria for success are based on the operational needs of the customer and it is mainly based on technical performance and the component agency's Concept of Operations (CONOPS). Based on this key input, the customers' requirements are translated into technical requirements with testable metrics of performance. These metrics of success, and how they will be assessed, are detailed in the test plan.

The ultimate goal is to ensure that equipment that will be deployed in the field is usable, effective, reliable, and maintainable over its operational lifetime. Thus, the time spent in DT&E assures that promising research and technology development transitions smoothly to the field and the end-users.

TSL's RDT&E personnel also perform testing of basic scientific principles, development of laboratory and field simulants and standards, testing of breadboard systems or components, testing of prototype systems, and testing of near-COTS or COTS systems to determine if systems meet the minimum requirements of the customer, and are ready to transfer over to TSL's IT&E testing.

Basic scientific principles are tested or measured utilizing expertise and advanced instrumentation at TSL to learn chemical or physical properties of materials (threats) or interactions with materials. This includes performing X-ray Diffraction and high energy X-ray/CT measurements on existing and home made explosives (HME) to determine the fundamental properties necessary for detection in COTS EDS systems. Similarly, ion chemistry measurements are collected to verify detection or interferences that may exist with ion mobility spectrometry (IMS) based explosives trace detection (ETD) systems.

Testing and development of Simulants and Standards are critical to the T&E of explosives detection systems both in the laboratory and field. TSL has developed many sets of bulk explosives simulants (for X-ray and CT systems) that allow testing of EDS systems without the need for the presence of dangerous bulk explosives, permitting systems to be tested in laboratory settings and for testing in the field for government customers. TSL has also developed a number of trace explosives standards for TSA, such as standards that are used for quality control (QC) checks on lab and fielded ETDs, trace particle standards to contaminate surfaces (baggage, laptops, vehicles, etc.) to verify proficiency of both the screener and ETD as a system, and a number of verification standards that other government performers or industry utilize to measure the efficiency of their ETD system.

Breadboard EDS systems, which are developed either at TSL, industry, academia, or a government laboratory, are tested or evaluated by TSL as part of a product developmental cycle. This testing allows TSL to utilize explosives threats to measure the technology's feasibility to meet the customers' defined requirements, or in some cases, general requirements to develop technology for S&T without specific agency requirements, but with minimum technology specifications. Often, Human Factors evaluations or assistance are brought into the process to provide early guidance with the end-users requirements for usability, interface, and suitability.

Prototype testing encompasses early developmental systems, which are typically provided by industry, academia, or government laboratories. Prototypes undergo testing to learn about detection capabilities and gaps, in order to improve and transfer the systems to the final production stage.

R&D Assessment of production stage prototypes is where TSL determines if a system is ready to be transferred over to IT&E for critical customer evaluation. This testing looks at the minimum detection requirements of the evaluated system, the human factors considerations for field use, issues with false alarms, interferences, and systems engineering requirements. Often this is where industry will get a chance to perform final product modifications to meet the intended customer's needs.

Certification Readiness Testing is a DT&E test conducted to provide quantitative evidence that a system meets (or fails to meet) the performance requirements prior to certification testing. This test is conducted in stages, in order to grow the candidate equipment performance so that it will be robust enough to have a good probability of passing the certification test. While certification may take only a few weeks to administer, Certification Readiness testing may take several months to a year of hard lab work with the industry partner to mature the candidate explosives detection system. Typically, the TSL presents increasingly harder Improvised Explosives Device (IED) concealments to candidate explosive screening equipment, and the vendor must, in turn, refine hardware and software to achieve detection of explosives with high levels of detection and low false alarm rates.

The results of all of the above RDT&E activities normally end up in technical documents which, along with oral debriefings, are provided to the customer. This provides them with clear and concise test plans, T&E data, summaries, comments and conclusions. With CRDAs, similar non-sensitive reports and debriefs are provided to the industrial partner to ensure they have gained the insight necessary to bring their product to the next step in the developmental process.

Coordination with other DHS components. TSL works closely with TSA in the translation of customer requirements into TSA technical requirements that have performance metrics of success, so that requirements are testable. The IT&E group provides the customer with high quality test data that guides decisions concerning operational robustness and detection capability of available systems. The IT&E group also regularly convenes working groups, contributes to IPT meetings, and produces rapid assessments to support TSA's efforts. The TSL has also shared its expertise with other DHS components, including the U.S. Coast Guard and U.S. Secret Service.

The TSL looks forward to contributing our expertise to the University Centers of Excellence (CoEs) in the areas of transportation and explosives. TSL personnel are working with the S&T Explosives Division to identify and evaluate potential research projects of interest, and TSL will be part of the proposal review chain. TSL has welcomed assorted undergraduate and graduate students as part of the DHS Scholars and Fellows program over the years. It should be noted that, prior to the establishment of the DHS CoEs, TSL has had a long and fruitful relationship with academia, via the Grants and Cooperative Agreement programs (FAA Grants Program). With these funding mechanisms, TSL has been able to work with academia to develop and perform RDT&E on novel next-generation explosives detection systems.

TSL and Technology Transfer

While the TSL performs testing and certification of technologies, it is the responsibility of TSA to define and judge readiness for deployment. Technologies passing certification are demonstrated to have efficacy, but do not necessarily demonstrate operational robustness. Deployment decisions are, in part, based on unique laboratory tests conducted at TSL that cannot be conducted in the field, along with operational utility evaluations conducted by TSA. If TSA encounters operational issues with a piloted or deployed system, TSL stands ready to provide subject matter expertise to understand the issue and assist in corrective action. Several examples of TSL's assistance in these situations are described with other technologies we have transferred below. Occasionally, TSL has taken the initiative to develop product support systems (e.g., the Image Quality phantom and trace quality control aids) to improve operational performance.

In terms of technology transfer, in addition to the clear technology transfer milestones that equipment certification and qualification play, the TSL offers continuous, daily support to enable this process. Some efforts are obvious, such as subject matter expert support for TSA programs, and some are more nuanced, such as refinements to federal security officer's training for explosives recognition, or training concerning use of an explosives detection system.

In addition to testing and certification, TSL continues to work with TSA as they plan for deployment. The Lab helps TSA develop appropriate training modules for newly deployed technologies. The TSL also continues to work with the TSA to aid in the monitoring and oversight of the configuration of each piloted or deployed system. As systems are upgraded to become more operationally robust, the TSL assesses the extent and nature of system changes, and occasionally calls for system recertification if changes may affect the performance criteria of the system. Finally, the deployment of explosives detection systems to the airports has created a secondary industry at the TSL: We have created high fidelity explosive simulants, test articles, quality control aides and other diagnostic tools that TSA uses to validate that the equipment or screeners are performing at the appropriate high standards.

TSL/TSA Transition Activities

TSL has worked with TSA to transition many programs that could improve transportation security. Examples of ongoing work include:

- TSL has been actively pursuing R&D relative to improving detection by **bomb sniffing dogs,** and provide training tools for canine handlers, training aids for canines and canine performance assessments for canines to TSA's National Explosives Detection Canine Training Program.
- TSL has a strong tradition of **Human Factors** expertise, and TSL's Human Factors group is currently involved with a number of projects in support of TSA. These efforts are critical to ensure that sophisticated equipment can be easily, safely, and effectively used by thousands of screeners in the field. Past activities included the creation of a selection test for X-ray screeners for TSA's Office of Human Capital; this was transitioned to TSA in 2001 and it has been used to hire all TSA screeners since then. Currently, the TSL Human Factors team are:
    - Providing a formal analysis of the so-called "re-screening problem" for a joint U.S.–Canadian Working Group, and looking at possible alternatives to re-screening of checked bags of Canadian origin at U.S. airports.
    - Working on the development of On-Screen Alarm Resolution (OSARP) procedures for Cargo, which presents new and different challenges to screeners using EDS.
    - Participating in a TSA pilot on the development of Cargo screening procedures for privately operated independent air carriers that acquire X-ray, Advanced Technology (AT) and Explosives Trace Detection (ETD) equipment.
    - Participating in TSA's Passenger Screening Program workgroup to develop measures of screening effectiveness. TSL also supports research on screener performance, screener attention focusing techniques, screener fatigue, and optimizing screener interfaces, which efforts are expected to contribute to TSA processes in the future.
    - Providing support to the TSL's Independent Test & Evaluation (IT&E) group assessments of Whole Body Imagers (WBI) for TSA. In the last year, Human Factors staff supported TSA with 14 separate WBI assessments examining the effects of multiple technologies, passenger poses, privacy settings, and threat sizes on threat detection capabilities.
    - Through a long-term research grant with the University of Central Florida, TSL's Human Factors experts have created a new and highly effective method for training TSA screeners to detect threats in carry-on bags. This new method has been shown to produce significant increases in threat detection in lab studies, and an initial pilot showed improved IED detection for screeners with this new training method. A comprehensive pilot study is being planned with TSA's Office of Technology Training to test 300 screeners across at least 20 different U.S. airports.
- TSL also has a tradition of supporting **mitigation efforts** and has assisted TSA's Office of Security Technologies with mitigation-related technology. In the late 1990's, TSL successfully blast-tested two hardened aircraft luggage container prototypes (**HULD**'s), which were subsequently certified to existing FAA airworthiness requirements. In 2006, the TSA's Office of Security Technology implemented the HULD Pilot Program in response to 9/11 Commission recommendations, the objective of which was to determine operational impact (security benefits, durability, maintenance, training impact, and cost) of any subsequent HULD implementation. During the course of the HULD Pilot, TSA placed a total of 25 HULD's into operational service trials; to date, 20 HULD's have been removed from service at predetermined intervals (between 100–350 flights), and TSL has blast-tested these in order to determine the effects of operational service on continued HULD blast resistance. Over the

next six months, TSL will complete explosive testing on the HULD's remaining in operational service.

Other Examples of Technology Transfer

TSL also provides technology transfer through its **Communications and Radio Frequency Identification** (RFID) group. These activities include:

- Cockpit-Crew Emergency Communications System Flight Tests. TSL provides expertise and flight tests to support TSA's Federal Air Marshals (FAMS) development of the FAMS Air-to-Ground Communications Architecture.
- Cargo RFID Seals Project. TSL is providing recommendations and test bed support for TSA's efforts to have a Cargo Screening System using RFID seals in place for 100 percent of all cargo shipments by August 2010.
- Canine Mass Transit Remote Sensor Project. This project is providing a pilot of a Canine Stand-off Situational Assessment for First Responders and was initiated by the TSA Deputy Administrator.
- Regional Maritime Security Coalition/Cargo Information Action Center. TSL contributed subject matter expertise and assistance with transference of Command, Control, Communications and Intelligence Network technology to Pacific Northwest Airports and Columbia River Seaports, linking TSA Federal Security Directors at Portland International and feeder airports with the U.S. Coast Guard, Customs and Border Patrol, FBI and State and Local Port Authorities and Emergency Management Centers.
- Atlantic City International Airport Testbed. TSL is working with the South Jersey Transportation Authority for in-situ RDT&E site for airport-related security technologies and systems.

Another major role that TSL plays in technology transfer is working with industry via **Cooperative Research and Development Awards** (CRDAs). The CRDA mechanism allows industry to mature their technology in partnership with the U.S. Government. TSL provides industry with a unique opportunity to perform RDT&E (laboratory evaluation) of its products with real explosive threats that are not typically available to the private sector, while at the same time providing industry with subject matter expertise to assist in the final development and maturation of technology. This allows Industry a path to mature technology that will meet performance standards required for DHS applications. To date, these activities have been limited due to lack of government funding and infrastructure/laboratory constraints.

Conclusion

In conclusion, the primary focus of the R&D and the test and evaluation at the TSL is to develop, mature, and transition technology to detect explosives. TSL combines a profound awareness of terrorist capabilities with penetrating insight about the operational environment. The Laboratory's close relationship with its customers allows us to fully understand customer needs and incorporate operational considerations into our R&D. By applying fundamental understandings of science, systems engineering, and test and evaluation protocols, the Laboratory is a unique national asset that is perfectly positioned to continue providing effective technology solutions for national security. The TSL stands proudly behind the fact that every piece of security technology presently deployed in the Nation's airports has at some point traveled through our doors. Whether it is during development, qualification, or certification, the hands and minds of the TSL team have played a role in all of today's technological solutions for the detection of explosives and conventional weapons in transportation security. Chairman Wu, Ranking Member Gingrey, and distinguished Members of the Committee, I want to thank you for giving me the opportunity to provide this testimony today.

BIOGRAPHY FOR SUSAN HALLOWELL

Dr. Hallowell is the Director of the Transportation Security Laboratory (TSL), a Federal Laboratory of the Science and Technology Directorate (S&T) of the Department of Homeland Security (DHS). This laboratory is responsible for researching, developing, and evaluating solutions to detect, deter and mitigate improvised explosive devices used against transportation systems. Prior to this, she was manager of the Explosives and Weapons Detection R&D Branch of the Transportation Security Laboratory.

Dr. Hallowell was recently recognized, in 2007, by Under Secretary Jay M. Cohen, S&T/DHS, with the Under Secretary's Award for Program Management. She supervised the transition of her lab within DHS from the Transportation Security Administration (TSA) to the Science and Technology Directorate. Dr. Hallowell moved the TSL in a new direction by reinventing it as a test and evaluation laboratory responsive to customers in all components of the DHS and to stakeholders in the public and private sectors. She has worked for the DHS, TSA, and FAA for over 15 years in the area of explosives detection research and development, and is an expert in the area of trace detection of explosives. She has written numerous publications and has received many awards in this area. Prior to working for the FAA, she worked as a research chemist for the U.S. Army, in the area of detection of and protection against chemical warfare agents, and technical measures supporting CW treaty verification.

She was granted a Doctor of Philosophy in Analytical Chemistry from the University of Delaware in 1989 for work in the area of biosensor development. She holds a Bachelor of Arts from Western Maryland College with a major in chemistry. Dr. Hallowell is a member of the American Chemical Society, the American Association for the Advancement of Science, the New York Academy of Science, National Association of Female Executives, and is an elected member of Sigma Xi, the society of research scientists.

Chairman WU. Thank you very much, Dr. Hallowell. Mr. Tsao, you may proceed.

STATEMENT OF MR. ADAM TSAO, CHIEF OF STAFF, OFFICE OF OPERATIONAL PROCESS AND TECHNOLOGY, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Mr. TSAO. Thank you very much, Mr. Chairman. Good afternoon, Mr. Chairman and distinguished Members of the Committee. I am honored to be here today to appear on behalf of the Transportation Security Administration to discuss our research, development, and testing needs and discuss how S&T supports our mission.

If it pleases the Committee, I would like to request that my written testimony be submitted for the record.

As you know, TSA operates at over 450 airports. WE operate screening operations 24 hours a day, seven days a week across six time zones. On a daily basis our 43,000 transportation security officers will see two million passengers or 1.8 million bags. My job as the Chief of Staff for Operational Process and Technology is to make sure the technology we feel provides the men and women of TSA the best opportunity in a very demanding environment against a determined foe.

As Dr. Hallowell pointed out, in 2006, the Department of Homeland Security consolidated all research, development, and testing functions of the component agencies within the DHS S&T Directorate. As such, TSA relies heavily on S&T to satisfy our basic applied and development research needs. At the same time, we maintain responsibility for operational testing and evaluation, operational integration, and deployment of new security technologies. We are also the ones that set the security strategy and that everybody works off of. We have a very strong relationship with each of the divisions of the S&T Directorate, but we have a particularly close affiliation with the Transportation Security Lab. Our histories go well back to when these activities were in the FAA. We depend heavily on, as Dr. Hallowell said, independent test evaluation at TSL. I know all the professors there, I know all the doctors, I know all the projects that they are working on. We talk on a daily basis. We have a very open dialogue on the information we need as well as the ways they can help us.

For each technology, we will identify the requirements that have to be met, and then the IT&E group will take those requirements, develop a test plan, test it, provide us the results. We will take these thorough and unbiased results and we will take them into consideration as we make our policy and investment decisions.

I think there were also some questions about how we participate in the S&T capstone integrated product teams. Last year I believe was the very first year for this process, and we engaged at a very high level. Administrator Holly himself co-chaired the first round of the explosives IPT with the Director of the U.S. Secret Service, Mark Sullivan. The process has been extremely valuable to us. Through the process, I think we have been able to better articulate our operational needs, not just our technical needs, but our operational needs to the rest of the department. Also, it has given us a fuller understanding of the needs of the other operating components, and it has given us opportunities to enter partnerships that we don't think we would have otherwise considered.

So, Mr. Chairman, again, thank you for the opportunity to highlight our progress in making aviation more secure, and I look forward to responding to your questions.

[The prepared statement of Mr. Tsao follows:]

PREPARED STATEMENT OF ADAM TSAO

Good afternoon, Chairman Wu, Ranking Member Gingrey, and Members of the Subcommittee. I am pleased to appear before you today on behalf of the Transportation Security Administration (TSA) to discuss the research, development, and testing/evaluation needs of the TSA and how the Science and Technology (S&T) Directorate supports the TSA mission.

TSA is the global leader in transportation security. We operate at airports across the country, 24 hours a day, seven days a week across six time zones. TSA employees screen more than two million passengers and 1.8 million of pieces of luggage daily. It is my job to provide the right technology to the field to support our vital security operations.

As an operating agency, we rely heavily on S&T Directorate to satisfy our basic, applied and developmental research and development. We have a strong working relationship within each division of S&T Directorate, with a particularly close affiliation with the Transportation Security Lab (TSL) in Atlantic City, New Jersey.

In 2006, the Department of Homeland Security (DHS) consolidated all research, development, and test and evaluation functions of its component agencies, with the exception of the U.S. Coast Guard, within the DHS S&T Directorate to achieve efficiencies through economies of scale. As required by the FY 2006 *DHS Appropriations Act,* the S&T Directorate assumed responsibility for the TSL from TSA. Since then, TSA has relied almost exclusively on the TSL for testing needs.

TECHNOLOGY AND THE PROCUREMENT PROCESS AT TSA

TSA works with the Independent Test and Evaluation (IT&E) group at TSL to develop programs that test whether or not a new technology meets its stated requirements. After completing testing procedures, the IT&E group provides TSA with thorough, unbiased testing results. We use the results to make policy and investment decisions.

TSA'S ROLE IN TECHNOLOGY TESTING

For each new technology, TSA develops and identifies the requirements that must be met for a procurement to proceed. The IT&E group within the TSL then takes these requirements and develops a testing program to determine whether or not a new technology meets the stated requirements. The role of TSA in designing these technology tests varies and is based on operational needs and the criticality of the technology and corresponding processes and procedures.

Both the TSL and the DHS S&T Directorate divisions have a strong working relationship with TSA. Their collective efforts are divided broadly into six areas.

The six areas are described in more detail, below:

- *Basic research* includes all scientific efforts and experimentation directed toward increasing knowledge and understanding in those fields of physical, engineering, environmental, social, and life sciences related to long-term national needs.
- *Applied research* includes all efforts directed toward the solution of specific problems with a view toward developing and evaluating the feasibility of proposed solutions.
- *Advanced development* includes all efforts directed towards projects that have moved into the development of hardware for field experiments and tests.
- *Operational testing* verifies that new systems are operationally effective, supportable, and suitable before deployment.
- *Operational integration* is the process by which TSA enables successful transition of viable technologies and systems to the field environment.
- *Deployment* is a series of actions following the determination that the: baselined product or system meets TSA's performance, operational, and user requirements and is accepted by the program manager and integrated product team; designated locations are selected, configured, and optimized for product/system integration into the screening operating system and the installed product/system passes acceptance testing at the designated location; logistics support is in place and all users are trained for operational use of the product/system. Only then is the product/system declared commissioned or cleared for use.

Additionally, DHS S&T Directorate is responsible for conducting basic and applied research, advanced development, and developmental test and evaluations. TSA maintains responsibility for operational testing and evaluation, operational integration, and deployment of new checkpoint screening technologies.

Integrated Product Team (IPT) Process

The S&T Directorate Capstone Integrated Product Team (IPT) began with 11 Capstone IPTs: Information Sharing, Border Security, Chem/Bio Defense, Maritime Security, Cyber Security, Explosives Prevention, Cargo Security, People Screening, Infrastructure Protection, Inter-operability, and Prep & Response.

At their February 26th, 2008 meeting, the Technology Oversight Group (TOG) determined that the Explosives Prevention Capstone IPT would be split into two IPTs—one focused on Transportation Security and the other on Counter-Improvised Explosive Devices (C–IED). As the result of this breakout, there are now a total of 12 Capstone IPTs. The Transportation Security Capstone IPT will be chaired by the Transportation Security Administration (TSA) and address priorities relative to venues (Airports, Mass Transit, and Maritime), checkpoints including air cargo, and explosives characterization and homemade explosives (HME). The C–IED Capstone IPT will be chaired by the Office for Bombing Prevention (OBP) and the United States Secret Service (USSS) with the objective of providing the technology to address the IED threat per Homeland Security Presidential Directive 19.

The IPTs program has been successful in many of its goals, including establishing budgetary funding priorities as part of the FY09 budget process and to prioritizing the research and development needs of TSA. As of November 2007, the Explosives Detection Division Capstone IPT has shown that TSA is able to articulate to DHS S&T Directorate a clear understanding of its science and technology needs to procure solutions that not only meet stringent detection thresholds, but also meet throughput requirements in support of the aviation sector.

TSA's involvement in setting user requirements for technologies developed or funded by S&T Directorate.

TSA no longer has primary responsibility for funding or managing the research and development of airport screening technologies. TSA does however remain primarily responsible for developing functional requirements for new technologies, including setting threshold standards for detection, and for conducting operational tests and evaluations of these technologies in airports. In the future, TSA's involvement will likely vary based on the maturity and criticality of the technology, as well as the operational rigor required to implement it.

Apart from the research and development efforts under S&T Directorate, TSA invests annually in engineering projects designed to improve or upgrade existing technology as new requirements are generated. In certain cases, existing technology is unable to support new requirements due to hardware or software constraints. In these instances, TSA undergoes a proposal solicitation process to evaluate new technology systems whose enhanced functionality will meet the revised requirements.

CONCLUSION

The needs of people must continue to drive the focus of transportation security. The American people and the traveling public require a transportation infrastructure that can be secured without the expense of unreasonable burdens. The people in our workforce require investments that will allow them to perform effectively and grow professionally. The people within our homeland security partnerships and network require cooperation, communication, and leadership. The strength of these relationships has been fundamental to our progress and must continue to remain a focal point as we move forward.

Mr. Chairman, thank you again for this opportunity to highlight the progress TSA has made in aviation security. I look forward to our continued work together and would be pleased to respond to your questions.

Chairman WU. Thank you very much, Mr. Tsao. Dr. Oxley, please proceed.

STATEMENT OF DR. JIMMIE C. OXLEY, PROFESSOR OF CHEMISTRY, UNIVERSITY OF RHODE ISLAND (URI); CO-DIRECTOR, URI FORENSIC SCIENCE PARTNERSHIP; CO-DIRECTOR, DHS UNIVERSITY CENTER OF EXCELLENCE IN EXPLOSIVE DETECTION, MITIGATION, AND RESPONSE

Dr. OXLEY. Thank you, Chairman Wu and Congressman Smith. I always like to talk to Smiths since I am married to one.

The question I was asked—three questions and the third question I think Dr. Hallowell has answered admirably, so I am going to start with the question about current state of research and explosives, and I gave first of all a very general answer because we do—all countries do current research in explosives. We have a very minor effort in the U.S. The NRC report that was published in 2004 estimated we had two dozen chemists working in energetic material new chemical synthesis. Now, I am talking about new military explosives, I am not talking about counter-terrorism type issues when I say that. We do work on formulating new devices to make our explosives safer to handle, more effective, and have longer or shorter lifetimes depending on what it is we are trying to accomplish. Device-centered research also occurs at the military labs. We are we are going on military labs and national labs. That is a general answer to a question of tell us about explosive research.

Governments all over the world put restrictions on military explosives. Despite that fact, if you look at the table I gave you, you will see that half of the explosive incidents have been with military explosives, in fact, not with commercial explosives, which may speak very well to the control that folks exert on commercial explosives.

You asked me a question about liquid explosives. Since solid explosives perform equally well to liquid explosives, we usually prefer to handle solid explosives, less handling problems. There is not new research, or very little, in new liquid explosives. However, there is much more literature on liquid explosives and what you see is terrorists pulling out that old literature and making use of things that are commercially available like hydrogen peroxide or nitro methane. These are not surprise materials, they are just taking advantage of what is already known.

We do need to have new research in detection across the board. The issues with detecting liquid explosives are related to (a), if manufacturers detect what they are asked to detect, and they have said we would like to know ahead of time what we are going to be asked next. They can't afford to have instruments detecting a threat that hasn't been asked for because it raises a false alarm rate. So you go right where you are asked and that type of detection.

The issues with liquids are we don't want to open the bottles, so it is a sealed container issue, and we have all the same issues if we have a well-filled solid to deal with. Detection issues must be addressed.

Concerning the chemicals themselves, we need some basic research in detonation to see what commodity chemicals that we are not aware of could be detonable. We need basic research in that area. There was a famous chemist in the World War II timeframe who said give me enough peanut butter and I will blow up the world, and we don't know if he is right or not about that one.

In this country we use 6.4 million metric tons of ammonium nitrate a year. Worldwide production is 39 million metric tons with nine million metric tons in transit. Urea is four-fold in terms of production and export of urea, and I have given you a table on those two issues. I consider those two the premiere explosive precursors to take a look at, and indeed the House and the Senate have passed the Secure Ammonium Nitrite law, and I believe that DHS is going to administer that. I think we need to look at a handful of explosive precursors for administrative control. That is very doable. We have been collecting this data since the 1980s, 30 years of data on who the end-users are. We just haven't really worked at making that a useful policy in terms of interdicting and following what happens from the manufacture to the end-user of specific precursors.

If I now move my 26 seconds to detection issues, across the board we have issues on getting the sample to the detector. We need basic particle surface studies in that area. Those are primarily for the detectors that require a molecule of the explosive to get into the instrument.

Our other detectors rely on a signal, an emission-type technology and those are bulk detectors and stand-off detectors. They have to have an emission signal. We need lots of development, but we need some basic research into what is physically, scientifically possible to do.

And my last point is that the manufacturers across the board and they come into my lab and they say, help us out. We want to know what is happening next. And if you want to engage the wonderful research that universities can do and the vendors themselves can do, we need a little better flow of information.

Thank you very much.

[The prepared statement of Dr. Oxley follows:]

PREPARED STATEMENT OF JIMMIE C. OXLEY

What is the current state-of-the-art in explosives research, especially as relates to homemade and liquid explosives? What are the key knowledge and capability gaps, and what types of research projects are needed to fill these gaps?

Little explosives research in the United States (U.S.) is focused on making new explosives, i.e., new chemicals. A 2004 National Research Council (NRC) report (Advanced Energetic Materials) wrote: *"The U.S. effort in the synthesis of energetic materials at present involves approximately 24 chemists, several of whom are approach-*

ing retirement." In the National Labs or Military Labs new formulations and new devices may be sought with goals of safer, more destructive, longer or shorter shelf-life. Device-centered research undoubtedly proceeds under government contract labs, as well.

Despite the fact that responsible governing bodies have emplaced various administrative controls to keep military explosives out of the hands of terrorists and criminals, international terrorism has relied heavily on these. Interestingly, military, rather than commercial, explosives have generally been their tool. This fact either speaks well of industrial safe guards or points the finger at State-sponsored terrorism.

The military has few applications for liquid explosives. Solid explosives perform equally well and have less handling and storage issues. For this reason, little new research in liquid explosives is performed. However, the old literature is rife with descriptions of liquid explosives, many of which are readily prepared and some of which, e.g., hydrogen peroxide and nitromethane, are commercially available. Liquid explosives are a detection challenge only because, in the past, detection equipment manufacturers had not been asked to detect them and because U.S. policy is not to open bottles. This does not mean liquids cannot be detected; the difficulty is the same as with any number of military or homemade explosives under these conditions. **Research in all areas of detection is required.**

The U.S. began to focus on homemade explosives after the bombing of the Murrah Federal Building (April 19, 1995). One tangible result was a 1998 NRC book *"Containing the Threat from Illegal Bombings."* In 2006 various governments began to use that report as guidance on explosive precursors. What has not been done is to follow the report recommendations for testing of materials to identify actual explosive precursors.

A methodical study is needed to identify the likely explosive precursors. We must probe the fundamentals of detonation to identify the energetic materials which could be made detonable with modest effort.

My criteria for homemade explosive threats are simple: (1) the required synthesis must be minimal—mix and use or mix and separate; and (2) large amounts of the precursor must be available and readily acquired so that large a bomb can be assembled. ["Large" bomb is part of the criteria with the rational that the bomb should be more of a threat than a gun or rifle.]

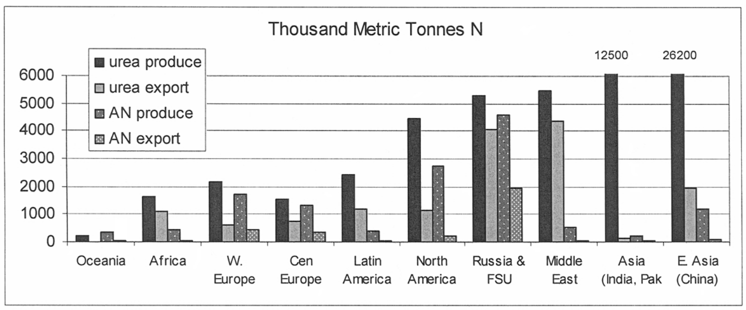
First on my list of homemade explosives are ammonium nitrate (AN) formulations and urea nitrate.

year	location	type of explosive	injured	dead	
1983	Beirut Marine & French Barracks	2 trucks, 12K lb C4?		300	
1988	Pan Am 103, Lockerbie Scotland	Semtex RDX/PETN		269	
1992	St Mary's Axe/Docklands, London	**1000's lb AN icing sugar**		3	*
1993	World Trade Center, NY	**1200 lb, urea nitrate**	~1000	6	
1993	Bombay 13 car & scooter bombs	RDX?	~1200	317	
1993	Bishops Gate, London	**3000 lb AN/icing sugar**	40	1	*
1995	Oklahoma City Federal building	**5000 lb ANFO**	~1000	168	
1996	Canary Wharf/Docklands London	**3000 lb AN/icing sugar**	39	0	*
1996	Manchester, UK	**1000's lb AN/icing sugar**	~200	0	*
1996	Khobar Towers, Saudi Arabia	0.5-30 K lb C4?	372	19	
1998	Kenya & Tanzania	2000 lb TNT & PETN	1000s	224	
2000	U.S.S. Cole, Yeman	1000 lb TNT & RDX	39	17	
2002	Limburg oil tanker	TNT?	12	1	
2002	Bali nightclub bombs	**chlorate**	**209**	**202**	
rob	Marriot Hotel, Jakarta	**chlorate**			
2003	Istanbul, Turkey	2 bombs	450	28	
2004	Madrid subway, 10 suicide bombs	gelignite in 4 locations	~600	191	
2005	London subway, 4 suicide bombs	**peroxide explosive**	~700	56	
2006	Mumbai, India railroad	7 explosions	625	190	

*PIRA bombs targeted economic loss rather than human loss; warnings were issued

The Provisional Irish Republican Army (PIRA) made kilogram-scale bombs mixing AN with icing sugar. Timothy McVey used AN with the traditional industrial fuel—diesel. In 2006 the U.S. manufactured ~6.4 million metric tons AN, its usage split between agricultural and industrial applications. Indeed, most commercial explosives are AN based. Worldwide about 39 million tons of AN are manufactured annually at about 200 chemical plants and about nine million tons of AN end up on the export market.

Worldwide urea production is significantly greater than AN—133 million metric tons annually and 31 million tons in export. Urea is used in agriculture, pharmaceuticals, NO_X abatement, and melamine synthesis (which with formaldehyde, forms resins used in adhesives, laminates, coatings and textile finishes). Urea is made from ammonia and carbon dioxide; typically plants producing ammonia produce urea as well. Ammonia is produced using natural gas and nitrogen from air; thus, areas with cheap natural gas make ammonia: China, Russia, Ukraine, the Middle East and Latin America. Urea plus nitric acid form urea nitrate; therefore, it is not surprising that urea nitrate, rather than AN, is frequently used by terrorists in the Middle East.



In investigating all avenues of preventing terrorist bombings, we should consider administrative controls on the most likely to be used homemade explosive precursors. **We should consider administrative tracking of a small number of precursor chemicals** (e.g., AN, urea, nitric acid, hydrogen peroxide, chlorates) **from manufacturer to end-user.** Such a program would involve identification of potential precursors and their legitimate place in society. It would require the cooperation of the manufacturers from the time the product left the factory through distributors, traders, and transporters to end-users. Such a system would not evolve overnight, but it should be possible with modern computer technology and international cooperation. Of course, it will not stop all diversions, any more than our present controls stop illicit use of military explosives. A 2007 NRC report *"Countering the Threat of Improvised Explosive Devices"* recommends among other areas of research: *"Perform case studies of actual IED construction and events to determine whether and how resource control might be implemented, with the eventual goal of developing the ability to model the connection between resources and the IED threat chain."*

How does current university research in the field of explosives and explosives detection contribute to technology development for aviation security? How is university research coordinated between institutions and with the Federal Government?

Failing to prevent a bomb from being made, we must consider detection of the bomb. Detection methodologies can be divided into those which require the actual explosive molecule to enter the instrument—these are called particle or vapor detection—and those which can detect characteristic emissions from the bulk explosive. Emission detection techniques can be passive, relying on a natural emission from the chemical, or active, probing the chemical with some sort of radiation to cause emission. Emission detectors can be differentiated as those having the potential to see, (1) with special detail, through sealed containers—check luggage or cargo—"bulk" detection; or (2) through the atmosphere at distances—"standoff" detection.

Trace techniques are at various levels of development. Even the commonly fielded ion mobility spectrometer (IMS) faces many operational challenges. For all trace techniques probably the toughest problem is getting the sample, the explosive molecule, into the detector. Solid explosives, generally, have low vapor pressure. Therefore, detection equipment attempts to sample microscopic particles, rather than vapor. To get a "detect" particles of explosive must be present; harvesting techniques must remove the particles from the surface; and the transfer technique must get the particles into the business end of the detector. Basic surface-particle interactions need to be studied. I understand the National Institute of Standards and Technology is working in this area and the Transportation Security Lab is funding further work.

Among emission detection techniques we find some of the most significant successes and the biggest gaps. As you know standoff detection and cargo screening need further research. As with other detection technologies we can expect to see imperfect systems fielded, but they can only improve with time, funding, and experience. One of the recommendations of the NRC report (*"Countering the Threat of Improvised Explosive Devices"* 2007) I would like to emphasize: **"Determine the fundamental physical limits on the active and passive detection of arming and firing systems, as well as the physical and chemical limitations for trace and standoff detection."**

One last gap I wish to highlight. If Universities are to significantly contribute their vast research skills to the National needs, we need a more open access to information in this area of threats and detection. I fully understand the need not to give terrorists information, but in many cases it is those who would help us whom we are keeping in the dark. Uniformly the technologies providers have asked: **"Increase communication to technology suppliers with respect to emerging threats, scenarios and threat levels." "Provide threat and precursor information to enable development of broad detection strategies."**

BIOGRAPHY FOR JIMMIE C. OXLEY

Dr. Jimmie C. Oxley is Professor of Chemistry at the University of Rhode Island (URI) and Co-Director of the URI Forensic Science Partnership and Co-Director of the recently announced DHS Center of Excellence in Explosive Detection, Mitigation and Response. Dr. Oxley has authored 80 papers on energetic materials. She worked with the FBI simulating the World Trade Center bombing, with Forensic Explosive Lab of the Defense Science and Technology Lab (UK) examining large fertilizer bombs, and with ATF/TSWG studying the behavior of pipe bombs. Dr. Oxley has taught over two dozen explosive short courses for various government labs and agencies and has served on five National Research Council panels: Commercial Aviation Security (1995–98); Marking, Rendering Inert, & Licensing of Explosive Material (1997–98); Chemical Weapon Destruction (1998–99); Advanced Energetic Materials (2001–02); Basic Research Needs to Interrupt the Improvised Explosive Device Delivery Chain (2005–08).

Chairman WU. Thank you very much, Dr. Oxley. Dr. Drury, please proceed.

STATEMENT OF DR. COLIN G. DRURY, DISTINGUISHED PROFESSOR AND CHAIR, DEPARTMENT OF INDUSTRIAL AND SYSTEMS ENGINEERING, STATE UNIVERSITY OF NEW YORK AT BUFFALO

Dr. DRURY. Thank you, Mr. Chairman, for inviting me to this hearing on such an important issue. I am a Human Factors Engineer from University at Buffalo, State University of New York. My research covers human performance in inspection systems from manufacturing industry through civil aviation to detection of threats on people. I have worked with people on the front lines such as TSA screeners and also been a member of committees on research in this field such as the NRC's committee on assessment of security technologies.

Human factors engineering uses data on the performance of humans, for example, security screeners; in complex systems, such as aviation security; to design better systems that make best use of the unique capabilities of both human and the automated devices to reduce error and increase throughput. There are three aspects of aviation security, three measures that we have already heard about. These are important, mis-threats, false alarms, and time taken to process each item. All of these translate into two overall measures, risk and delay.

To integrate human factors engineering into the design of future technological systems, we can use successful design techniques from other areas, design of military systems, civil aviation cockpits, chemical and nuclear facility control rooms have all be done.

The first step is to recognize that humans are going to be present in security systems. The traveling public is no more trusting of completely automated security systems than they are of unmanned airliner cockpits. The issue is not whether we can eliminate the human but how best to use the human who is going to be there.

An example is the in-line check baggage inspection system at many airports. It is based on 3–D scanning of each bag. Automation is used to highlight those areas that contain a potential threat. This is a search function. The highlighted bag is shown to the human operator who has to mark it for further inspection or pass it. This is a decision function. Humans are relatively quite reliable in decisions whereas machines are much more reliable in search. So this is quite sensible.

In general, automation is allowed to perform rapidly within strict rules while humans provide the flexibility to respond when the rules don't apply.

The next steps after this are to design specifically for the humans. They human interface with the technology, the training programs, they interface between people, for example, at check points. There are standard techniques in human factors that have been used in these other fields to do this.

Currently, the TSA has professionals within the human factors engineering area with expertise at the Transportation Security Lab. And all of these are currently listed as members of the Human Factors and Ergonomics Society, but they have been working extensively with researchers and manufacturers on improvements to the interfaces as well as longer-term research studies such as developing selection procedures for screeners and human problems in container security. They have also funded some more fundamental studies of human factors engineering and security. For example, I have got a one-year grant from them at SUNY.

Could more be done? Certainly. The last time I visited a manufacturer which was a couple years back, there was little evidence of using human factors engineering professional expertise in design of systems. Without early involvement of human factors engineering, the human in the system may not make the ultimate decisions resulting in increased risk and passenger delay.

We can measure the effectiveness of human factors engineering as we have been talking about in security equipment in two ways. The first way is to evaluate whether the machine shows evidence of having human factors engineering used. The second way and the third way is to evaluate the performance of the whole system, the human plus the equipment. And if this is done correctly, with performance measures and observations measures, we can measure the errors and performance times to get a figure of merit for the system. But the observations provide the locus of any performance defect, so we can see perhaps why these things are happening.

To sum up, overall there is really no down-side to using human factors engineering in the design of security systems. Without it predictable performance lapses can occur, leading to increased risk and passenger delays. The additional cost of incorporating human factors engineering early in the process has been found in aviation and military domains to be rather low.

Thank you for your time.

[The prepared statement of Dr. Drury follows:]

PREPARED STATEMENT OF COLIN G. DRURY

In your testimony please answer the following questions:

1. *What role does human factors engineering play in the design and testing of aviation security technology? How well do current aviation security technologies incorporate human factors engineering and human-technology interface principles?*
2. *How does human factors engineering impact the effectiveness of these technologies to detect or deter threats? What are the possible detrimental effects of not involving human factors engineers throughout the technology design process?*
3. *How should the Transportation Security Administration and Transportation Security Laboratory test and evaluate whether human-technology interface principles have been properly applied in the design and manufacturing of aviation security technologies?*

I am a Human Factors Engineer from University at Buffalo: State University of New York. I have spent much of my life in research and intervention in the area of human performance in inspection systems. This started in manufacturing industry (cars, electronics, glass products) but transitioned to aviation inspection of civil airliners and inspection of people and goods for security threats. My CV provides samples of the technical papers published in inspection for manufacturing, aircraft maintenance and security. This work, as with all Human Factors Engineering (HFE), involved working with people on the front lines (e.g., maintenance technicians, TSA screeners) as well as membership in committees on research and development in this field (e.g., the NRC's *Committee on Assessment of Security Technologies in Transportation,* and the FAA's *Research, Engineering and Development Advisory Committee*).

Human Factors Engineering (HFE) is a discipline dating from World War II that uses data on the performance of humans (in our case security screeners, airline passengers) in complex systems (in our case aviation security) to design better systems that make the best use of the unique capabilities of both humans and automated devices while reducing the impact of their respective limitations. The diagram of the airport security system used by the National research Council (Figure 1) shows the level of complexity and the numerous places where humans can both make errors and act to prevent errors.

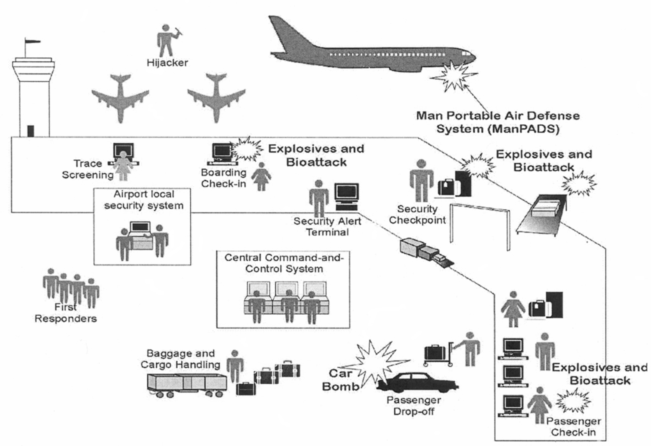


Figure 1: Airport Security System, from National Research Council, 2007, p 14.

Standard texts in this area include Wickens, Lee, Liu and Gordon-Becker (2002). It has a record of designing systems to prevent human error and inefficiency, beginning in the military but subsequently moving into civil aviation and industrial systems. If HFE is not used, then often the system errors only become apparent when the system is put to operational use, for example the control room and training deficiencies at the Three Mile Island nuclear power station.

There are three aspects of aviation security inspection performance where humans have a large impact: missed threats (failure to stop a threat), false alarms (stopping a person/item that is not a threat) and time taken to process each passenger or baggage items. All translate into two system performance measures: risk and delay. HFE applied to aviation security inspection can, and has, addressed each of these. A good example is the Threat Image Projection System (TIPS) which presents images of guns, knives and IEDs to screeners performing an X-ray screening task. This counteracts the known human tendency to detect fewer threats when there is a low probability that any single item contains a threat. TIPS has the added benefit of providing embedded training and performance measurement for screeners. TIPS act as a motivator to screeners, as well as reducing monotonly, but it must be technically well-executed to prevent non-threat-related artifacts from cuing the screener that a TIPS image is being displayed. HFE tells us that these three aspects of performance trade off against each other. In any given system, fewer missed threats are accompanied by more false alarms (e.g., National Research Council, 2007, p. 25; McCarley et al., 2004). Also there is a Speed-Accuracy Trade-Off in that fewer threats are detected if insufficient time is devoted to the inspection of each person or item (Drury, Ghylin and Holness, 2006). Mathematical relationships can be used to model these trade-offs (Drury, Ghylin and Schwaninger, 2007), so that we can deploy security systems to meet specific needs. The interaction between the screener and the technology is not the only application of HFE to security systems: passengers too interact with the system. Obvious examples are queuing at airports, where the screening delays turn into passenger dissatisfaction (Marin, Drury, Batta & Lin, 2008), and HFE input into helping novice passengers deal with the complexities of required tasks in a timely manner.

To integrate HFE into design of future technological systems for aviation security, successful design techniques from other domains can be used. HFE has been successfully applied to the design of most military systems, to civil aircraft cockpits and to chemical and nuclear facility control rooms. The issue in all of these, as in aviation security, is to use data on human behavior to blend the automation and human components of a system so that human and automation each do what they do best. This is known as Allocation of Function (e.g., Hollnagel and Bye, 2000; Lee and Moray, 1992) and has been applied to inspection tasks previously (Hou, Lin and Drury, 1993)

The first step is to recognize that humans will be present in all security systems. The traveling public is no more trusting of completely automated security systems than they are of unmanned airliner cockpits. The issue is not whether we can eliminate the human, but how best to use the human who will be there. An example is the in-line checked baggage inspection systems at many airports. The technology is based on 3–D scanning of each bag to build a 3–D image of the bag. Automation is used to locate areas of potential threat (e.g., atomic numbers associated with explosives) within the whole bag, i.e. a search function. The bag image with the potential threat area highlighted is displayed to the operator who then has the decision function of choosing to pass the bag as “no threat” or mark it for further screening, typically hand search (which is itself not error free). This allocation of functions between the automation (search) and the human (decision) capitalizes on known strengths and limitations of humans in inspection (Hou, Lin and Drury, 1993). For humans the search function is consistently quite error-prone, while the decision function (with suitable training and aiding) can be reliable (Drury and Spencer, 1997). Overall, automation provides the ability to take rapid and consistent action within strict rules, while humans provide the flexibility to respond when the rules do not apply (e.g., Parasuraman, Sheridan and Wickens, 2000).

Having decided what roles humans and automation should play in each future system, the next steps involve designing specifically for the human. This means working from the human outwards rather than the technology inwards. It means devising the interfaces between the human operator and the technology, identifying the training (and retraining) required for top performance, and designing the interfaces between the front-line operator (e.g., screener) and others in the system (e.g., other front-line personnel, supervisors, law enforcement officers, etc.). Interface design uses standard HFE methods with data and models of human functioning (from sensory and cognitive capabilities to physical size and strength) and applies it to design of the physical interface and computer software (Wickens et al., 2002). Applications range from comfortable seating and sightlines (e.g., for X-ray screeners) to human computer interaction (e.g., display and response logic for body scans or checked baggage inspection) using standard texts, e.g., Helander, Landauer, & Prabhu (1997). Training design can be based on well-known adult learning techniques. Design of human—human interaction can use techniques from either Crew Resource Management (CRM) or socio-technical systems design (STS) as found in Helmreich, Merritt & Wilhelm (1999) and Taylor and Felten (1993) respectively. Many comprehensive systems exist for including the human in the design of complex systems, e.g., Cognitive Work Analysis (Vicente, 1999) and even earlier in Systems Analysis (Singleton, 1974). All of these methods will help eliminate errors in the final human-machine system.

Currently TSA has HFE professional expertise at the Transportation Security Laboratory, although none of these professionals are currently listed as members of the Human Factors and Ergonomics Society. They have worked with researchers and manufacturers on short-term improvements to the interfaces as well as on longer-term research studies such as developing selection procedures, socio-technical systems design of the whole security checkpoint and human problems in container security. They have also funded some more fundamental studies applying cognitive science to security modeling, including a one-year grant to me at UB:SUNY as listed in my disclosure letter to the committee. Could more be done? Most certainly. There are new ideas where HFE expertise can be incorporated early in the design process. A recent example is data fusion, that involves humans as one of the many sensors whose data is fused to enhance decision-making, (e.g., NRC, 2007). Most manufacturers and researchers still see the physics and chemistry of detection as central, with design for the human in the system limited to training design and design of the computer screens and response keys. The last time I visited a manufacturer (for the NRC Committee) was several years ago but there was no evidence of using HFE professional expertise in systems design. Without early involvement of HFE, the human in the system may not make optimum decisions, and by then only small changes can be made to the system at evaluation time. This does not ensure that risk and passenger delays have been minimized.

How can we measure the effectiveness of HFE design in security equipment? This is important to ensure that we are indeed designing the systems optimally. Two alternatives are possible: examining the equipment for evidence that HFE has been used in its design, and/or evaluating the complete system (equipment plus human) and analyzing its performance and errors. Both have been used successfully. A design checklist can be rather simplistic for complex equipment embedded in operational systems, but the design procedures can also be reviewed to see how the deasign team took HFE into account. The TSL has used such a checklist to assist machinery designers in applying HFE to their products. The current, and recommended, method is to evaluate the performance of the complete system in as close as possible to real use conditions. Here we can measure the errors and performance times and also observe and interview users. This evaluation gives a figure of merit for the system (misses, false alarms, delays) and uses behavioral observation and structured interviews to examine the locus of any performance deficits.

Overall, there is no down-side to using HFE in design of security systems. Without it, predictable performance lapses occur, leading to increased risk and passenger delays. The additional cost of incorporating HFE has been found in aviation and military domains to be low.

References

Drury, C.G., 1994, Function allocation in manufacturing. In S.A. Robertson (ed), *Contemporary Ergonomics 1994* (London: Taylor & Francis, Ltd), 2–16.

Drury, C.G., Spencer, F.W. (1997). Measuring human reliability in aircraft inspection. *Proceedings of the 13th Triennial Congress of the International Ergonomics Association '97,* Tampere, Finland, Vol. 3, 34–35.

Drury, C.G., Ghylin, K.M. & Holness, K. (2006) Error analysis and threat magnitude for carry-on bag inspection. *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting—2006,* 1189–1193.

Drury, C.G., Ghylin, K.M. & Schwaninger, A. (2007) Large-Scale Validation of a Security Inspection Model, *Contemporary Ergonomics* 2007, Taylor & Francis, London.

Helander, M., Landauer, T. & Prabhu P. (1997) *Handbook of Human-Computer Interaction* (2nd Edition) Amsterdam, North Holland.

Helmreich, R.L., Merritt, A.C., & Wilhelm, J.A. (1999). The evolution of Crew Resource Management training in commercial aviation. *International Journal of Aviation Psychology,* 9(1), 19–32.

Hollnagel, E., and Bye, A. (2000). Principles for Modeling Function Allocation. *Int. J. Human-Computer Studies.* Vol. 52, pp. 253–265.

Hou, T.-S., Lin, L. and Drury, C.G. (1993). An Empirical Study of Hybrid Inspection Systems and Allocation of Inspection Function. *International Journal of Human Factors in Manufacturing,* 3, 351–367.

Lee, J. and Moray, N. (1992). Trust, control strategies and allocation of function in human machine systems. *Ergonomics* 35(10), 1234–1270.

Marin, C.C. Drury, C.G., Batta, R. and Lin, L. (2007) Server Adaptation in an Airport security System Queue. *OR Insight,* 20.4, 22–31.

McCarley, J.S., Kramer, A.F., Wickens,C.D., Vidoni, E.D. & Boot, W.R. (2004) Visual Skills in Airport Security Screening. *Psychological Science,* 15(5), 302–306.

National Research Council (2007) *Fusion Of Security System Data To Improve Airport Security,* The National Academies Press, DC.

Parasuraman, R., Sheridan, T.B. and Wickens, C.D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics—Part A: Systems and Humans,* Vol. 30 (3), May 2000.

Singleton, W.T. (1974) *Man-Machine Systems* (Penguin, UK).

Taylor, J.C. and Felten, D.F. (1992) *Performance by Design,* Prentice Hall.

Wickens, Lee, Liu and Gordon-Becker (2002) *Introduction to Human Factors Engineering* (2nd Edition), Prentice-Hall, NJ.

BIOGRAPHY FOR COLIN G. DRURY

PROFESSIONAL PREPARATION

University of Birmingham, Ph.D., Engineering Production specializing in Ergonomics, 1968

University of Sheffield, B.S., Honors Physics, 1962

APPOINTMENTS

2007–present—SUNY Distinguished Professor, University at Buffalo, SUNY.

2002–2007—UB Distinguished Professor, University at Buffalo, SUNY.

1979–2002—Professor of Industrial Engineering, University at Buffalo, SUNY.

1976–1979—Associate Professor of Industrial Engineering, SUNY–Buffalo.

1972–1976—Assistant Professor of Industrial Engineering, SUNY–Buffalo.

1968–1972—Manager of Ergonomics, Pilkington Brothers Ltd., St. Helens, England.

1967–1968—Visiting Assistant Professor of Industrial Engineering, UMass at Amherst.

1962–1964—Research Engineer, Motor Industry Research Association, Nuneaton, England.

INSPECTION ACTIVITIES and MAJOR AWARDS

Colin Drury has been actively researching inspection tasks since the 1970s, for which he was awarded the Bartlett Medal of the Ergonomics Society in 1981. In the 1980s he started applying this to aircraft safety inspection through a series of FAA grants, resulting in successful Best Practices Guides to several Non-Destructive Inspection techniques used in aviation. For this work he was awarded the FAA's Excellence in Aviation Research Award in 2005, and the Human Factors and Ergonomics Society's A.R. Lauer Award in 2005. In the 1990s he applied this to security inspection with contracts from the Air Transport Association and Atlanta's Hartsfield Airport. He has served on several NRC/NAS committees and panels on aviation security technology, during which he has studied the security systems at many airports in USA and Europe. For this work with TSA and FAA he was awarded the American Association of Engineering Societies' Kenneth Andrew Roe Award in 2006. He is currently a member of INTERTAG, the international human factors coordinating group on aviation security. In 2003 he was awarded a TSA grant to form the Research Institute on Safety and Security in Transportation (RISST) at University at Buffalo. In 2008 he was elected as Honorary Fellow in The Ergonomics Society, UK.

PROFESSIONAL PUBLICATIONS (OUT OF OVER 300)

(i) PUBLICATIONS MOST RELATED TO TESTIMONY

1. Marin, C.C. Drury, C.G., Batta, R. and Lin, L. (2007) Server Adaptation in an Airport security System Queue. *OR Insight,* 20.4 22–31.
2. Drury, C.G. (2001). A unified model of human security inspection. *Proceedings of Third International Aviation Security Technology Symposium,* Atlantic City, NJ, 27–30.
3. Drury, C.G., Hsiao, Y-L., Joseph, C., Joshi, S., Lapp, J. and Pennathur, P.R. (2008) Posture and performance: sitting vs. standing for security screening, *Ergonomics,* 51.3, 290–307.
4. Drury, C.G., Ghylin, K.M. & Holness, K. (2006) Error analysis and threat magnitude for carry-on bag inspection. *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting—2006,* 1189–1193.
5. Ghylin, K.M., Drury, C.G., Batta, R and Lin, L. (2007) Temporal Effects in a Security Inspection Task: Breakdown of Performance Components *Proceedings of the Human Factors and Ergonomics Societ 51sty Annual Meeting—2007,* 93–97.
6. Drury, C.G., Ghylin, K.M. & Schwaninger, A. (2007) Large-Scale Validation of a Security Inspection Model, *Contemporary Ergonomics* 2007, Taylor & Francis, London.
7. Ghylin, K.M., Drury, C.G., & Schwaninger, A. (2006). Two-component Model of Security Inspection: Application and Findings. *Proceedings of the 16th World Congress of the International Ergonomics Association,* 2006.
8. Panjawani and Drury, C.G. (2003). Effective interventions in rare event inspection. *Proceedings of the Human Factors and Ergonomics Society 47th Annual Meeting,* 2003, 41–45.
9. Drury, C.G., Saran, M. and Schultz, J. (2004) Temporal Effects in Aircraft Inspection: What Price Vigilance Research? *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting—2004,* 113–117.
10. Drury, C.G. (2001). Human Factors and Automation in Test and Inspection, In G. Salvendy, *Handbook of Industrial Engineering,* Third Edition, Chapter 71, John Wiley & Sons, New York, 1887–1920.
11. Hong, S.-K. and Drury, C.G. (2002). Sensitivity and validity of visual search models for multiple targets. *Theoretical Issues in Ergonomic Science,* 1–26.
12. Drury, C.G., Green, B.D., Chen, J. & Henry, E.L. (2006) Sleep, sleepiness, fatigue, and vigilance in a day and night inspection task, *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting—2006,* 66–70.

(ii) OTHER SIGNIFICANT PUBLICATIONS

1. Karwan, M., Morowski, T.B. and Drury, C.G. (1995). Optimum Speed of Visual Inspection Using a Systematic Search Strategy. *IIE Transactions,* 27, 291–299.
2. Hou, T.-S., Lin, L. and Drury, C.G. (1993). An Empirical Study of Hybrid Inspection Systems and Allocation of Inspection Function. *International Journal of Human Factors in Manufacturing,* 3, 351–367.
3. Baveja, A., Drury, C.G., Marwan, M.H. and Malon, D.M. (1996). Derivation and Test of an Optimum Overlapping-Lobes Model of Visual Search. *IEEE Transactions on Systems, Man and Cybernetics—Part A: Systems and Humans,* 26(1), 161–168.
4. Drury, C.G. (1997). Ergonomics and the quality movement (The Ergonomics Society 1996 Lecture). *Ergonomics,* 40(3), 249–264.
5. Mazumder, S., Drury, C.G. and Helander, M. (1997). Binocular Rivalry as Aid in visual search–r—95/539A, *Human Factors,* 39(4), 642–650.
6. Drury, C.G. (2001). Inspection. In W. Karwowski, (Ed.), *International Encyclopedia of Ergonomics and Human Factors,* Taylor and Francis, Inc., 1249–1253.
7. Drury, C.G. (2001). Human Factors and Total Quality Management. In W. Karwowski, (Ed.) *International Encyclopedia of Ergonomics and Human Factors,* Taylor and Francis, Inc., 1246–1248.
8. Drury, C.G. (2005). Inspecting, Checking and Auditing, particularly of Human Factors. In G. Salvendy (ed.), *Handbook of Human Factors and Ergonomics,* J. Wiley & Sons, Inc., NJ.

9. Drury, C.G. (1992). Design for Inspectability. In M.H. Helander and M. Nagamachi (ed), *Design for Manufacturability: A Systems Approach to Concurrent Engineering and Ergonomics.* Taylor & Francis, Ltd., London.
10. Drury, C.G. (2003). Service Quality and Human Factors. *AI and Society,* 17(2), 78–96.
11. Drury, C.G. (1985). Stress and Quality Control Inspection. Chapter 7 of *Job Stress and Blue Collar Work.* C.L. Cooper and M.J. Smith (Eds.) John Wiley, Chichester, UK.
12. *Human Reliability in Quality Control.* (1975) C.G. Drury and J.G. Fox (Eds.), Taylor & Francis, London.
13. Drury, C.G. (2000). Global Quality: linking ergonomics and production. *International Journal of Production Research,* 38(17), 4007–4018.

SERVICE ON NATIONAL RESEACH AND ADVISORY COMMITTEES

1. National Academy of Sciences/National Research Council
    - Human Factors Committee, member, 1997–2004
    - Panel on Musculo-Skeletal Disorders, co-chair, 1998
    - Workshop on Work-related Musculoskeletal injuries: The research base, 1998, co-chair of the steering committee
    - Panel on Musculoskeletal Disorders and the Workplace: Low Back and Upper Extremities, member 1999–2001
    - Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, member 1992–1996
    - Committee on Evalauation of Chemical Events at Army Chemical Agent Disposal Facilities, member 2000–2002
    - Committee on Monitoring at Army Chemical Agent Disposal Facilities, member 2004–2005
    - Committee on Deployment of New Technology for Aviation Security, member, 1999–2004
    - Committee on Assessment of Security Technologies in Transportation, member, 2004–
    - Committee Continuing Operations at Army Chemical Agent Disposal Facilities, member 2006–
2. National Aeronautics and Space Administration, Chair, Science and Technology Working Group (STWG), 2000–2004
3. Transportation Security Administration, Scientific Advisory Panel, 2004–2005.
4. Federal Aviation Administration Research, Engineering and Development Advisory Committee (REDAC), member 2002–2007, Chair Human Factors Committee, 2003–2004.
5. International Aviation Security Human Factors Technical Advisory Group (InterTAG), member, 2004–

DISCUSSION

Chairman WU. Thank you very much. At this point, we will open our first round of questions, and the Chair recognizes himself for five minutes.

It is not that we don't have better things to do, but we do fly a lot. We Members of Congress do fly a lot, and we, at times, well, we speculate about all sorts of things. And after September 11, one of the things we speculated about is if you were to bring down an airplane, how would you do it? And top of the list for those of us in the Oregon delegation was a flammable liquid. That was in the fall of 2001 or the winter of 2002, and yet my recollection is that restrictions on liquids or the focus on liquids didn't occur until much more recently.

Now, you all are responsible for implementation and for research. We Members of Congress are not scientists. We are not reputed to be very smart, but how come we were thinking about something that TSA didn't start looking for until much later, and was research being done in this field prior to the implementation of limitations on liquids on board airplanes? Dr. Hallowell, Mr. Tsao, would you care to handle that first?

Dr. HALLOWELL. Well, first off, I believe the FAA prohibits handling flammable liquids on aircraft, and I know this because they took a whole bunch of rum from me coming back from an island.

Chairman WU. Well, I know the FAA prohibits that, but there was no method of—there was not an active search or prohibition—I mean, the prohibition might have been in place but I believe until relatively recently you could take a large bottle of something, whether it is rum or water, on board an airplane. When did the ban go into place where it was actually looked for by the TSA?

Mr. TSAO. We actually implemented the ban on August 10th of 2006.

Chairman WU. So that is a four and one-half year window——

Mr. TSAO. Yes, sir.

Chairman WU.—from September 11 to the ban.

Mr. TSAO. Yes, sir.

Chairman WU. Did folks think that that might be a threat?

Mr. TSAO. We did look at, and some of that predated my time at the agency, but we did look at the various threats to civil aviation and the threats of—whenever we look at risk, we really look at three components of risk. One, what is the threat stream? Is there an adversary interested in this? What is the adversary's ability to carry that out? Two, what is the consequence? What will happen if the adversary, and three, what is the inherent vulnerability of the system? So I think when you start looking at those factors, the threat of a flammable liquid taking down an aircraft is relatively low compared to other threats at the time. During August of 2006, it was determined that there was a new threat using a liquid explosive which was judged to be powerful enough to cause catastrophic damage.

Chairman WU. Forgive me, Mr. Tsao, if I am, you know, imagining things that can't happen, but it was another Member of our delegation, one much more senior—who is much more senior than I and with substantial aviation experience. The methodology would just be to take a bottle of gasoline, run down the aisle, and have one person behind you ignite the stream and the consequences would be pretty dire.

Mr. TSAO. Relative to other threats we are facing, sir. We believe that is a lower threat.

Dr. OXLEY. Chairman, may I say something?

Chairman WU. Please.

Dr. OXLEY. The difference between a deflagration, a burn, and a detonation is huge.

Chairman WU. Yes.

Dr. OXLEY. And I think that is what Mr. Tsao is telling you, that relatively speaking, the detonation threat that came in late 2006, the summer of 2006, was substantial.

Chairman WU. But if you have a burning cabin, I mean, that is a bit of a concern in an airplane, isn't it?

Dr. OXLEY. Certainly, and there is a whole group I have run into in—I don't know if they are FAA or TSA—that is looking at protecting aircraft from fire.

Chairman WU. Well, you know, the point of the question is not what has happened in the past. The point of the question is are you properly identifying threats for the future?

Mr. TSAO. We believe so. Again sir, take three parts of our methodology. What are the adversaries looking at, what are the inherent vulnerabilities to the system, and what are the potential consequences, primary and secondary?

Dr. OXLEY. And I wanted to add that prior to the overt ban on liquids, our lab was already doing research because we had been asked by a federal agency to do so. So this was not a surprise that these liquids were a possibility. It was just a prioritization. If everything is looked at once, you miss the high priority items.

Chairman WU. I understand, at least among the Oregon delegation, the flammable liquid scenario is our number one, and we found it rather curious that that was not on other folks' list. Dr. Oxley, what you had to say is the most comforting thing that I have heard thus far.

I recognize the Member from California for five minutes—Nebraska. My apologies. It is California without an ocean.

Mr. SMITH. I will get back to you on that.

Chairman WU. California with a football team.

Mr. SMITH. Needing a little extra work there. But thank you, Chairman Wu, and witnesses.

Again, I am not an expert. You are. I guess if routine or repetition makes us experts, some of us could be in terms of airline security.

I think Dr. Drury you might be best to respond to this, but how do you decide, you know, what the threshold is for a discretionary decision as someone is—as a TSA worker—is going through a check point?

Dr. DRURY. The rules are fairly clearly written by this TSA and TSL. But the point about having the human in there is that they make fairly routine decisions pretty well. The better you can organize it so that they are doing what is called rule-based work so they follow a set of rules, just as in landing an airliner. You have a set of rules, a rule-based decision system. So you have a pilot in there who can look for things that aren't covered by the rules, look for the unusual things. The person who found explosives coming over the border into Washington State, for example, customs agent, security agent there, this was a beautiful piece of human following things that weren't directly part of the thing you have to do every time. So humans have two functions, one is to follow a set of rules where those rules apply, and they do that reasonably well. They don't do it perfectly but neither do machines. And the other one is to bring their unique human capabilities into there of reasoning it out so it is not a rule-based decision. It is called a knowledge-based decision where you work things out from first principles. Yes, this looks suspicious. I will do this.

Mr. SMITH. So there is—I mean, I don't expect a quick formula necessarily, but I am curious as to how or what the approach is. Sometimes what would appear to be common sense to me doesn't appear to be common sense as I go through a checkpoint at an airport. And I am just using my own anecdotal experience from repetition. But can you explain how perhaps they eliminate some of those decisions?

Dr. DRURY. Many of them are rules they have to follow. For example, when they check on your ticket and so on. So there are strict rules they have to follow here. And at the checkpoint, they have got higher levels of authority. They can pass things up, too, if needed. So they are not entirely on their own. But they are the first people who can trigger a response. So if they trigger a response, the system can move ahead. If they don't trigger a response, it doesn't. So in some ways it is reasonably optimum for them to make some false alarms to make sure that they have got, they have covered the things that are unusual.

Mr. SMITH. For example, and I hate to get hung up on details here, but a container that its ultimate capacity exceeded the restriction but its obvious contents are far below the limits and yet the whole line is stopped, the passenger is asked how much exactly or letting them know that it is going to go in the trash or whatever the case is. I mean, to me that could be avoided. Am I missing something?

Dr. DRURY. No, I have had exactly the same thing where I was carrying a small amount of liquid in a larger container and they were following rules. You know, their first line of defense is to follow the rules, and if you look at the consequences for not following them, you can see why people might wish to follow them because they could be checked up on easily and somebody could say—you or I could be a person going through testing them and saying do they follow the rules. So in this case, they wouldn't. Does it make sense on every occasion? I don't think so, but the question is which error do you want to make? And I think the error of potential inconvenience of passengers as I was and presumably you were is probably less than letting something through that could be construed as a threat.

Mr. SMITH. Thank you. Mr. Tsao, if you wouldn't mind elaborating perhaps on how the rules are made? And also, would someone with more seniority or more authority be able to just automatically pass over something such as that? Maybe if you could speak to uniformity as well?

Mr. TSAO. Certainly. I think one of the real difficulties for our screening workforce is again the number of people we see in any given day, two million passengers a day going through various different types—coming with very different travel patterns, you know, whatever they are coming through. It is difficult for us to train for every single opportunity or exception that may occur. And so giving the screeners leeway which we are leaning towards is very difficult to train. We are moving toward a system where instead of being a rules-based system, you focus more on your interaction with the passenger. But again, that is very complicated for us to initiate and we are just starting that. But it really comes down to volume. You may have two ounces of water in a 16-ounce bottle, we will let you through, but does that mean the next 400 people in line do the same thing? So it becomes a process where you have got to draw the line somewhere. And then unfortunately the next time you will know, don't come with a 16-ounce bottle with only two ounces of liquid in it. That is the only way we can keep the lines moving. It is the only way we can have a consistency of product.

Mr. SMITH. And so you would argue then that they actually end up doing it faster? And I will accept that. That does make——

Mr. TSAO. In the long run, yes, sir.

Mr. SMITH.—sense.

Mr. TSAO. Again, if you have too many exceptions, you know, every time you have got to call over a supervisor to answer certain things, is it worthwhile for the traveling public? Is it worthwhile on a security basis to again start making exceptions to every possible scenario that can go through?

Mr. SMITH. Is it conceivable that the smaller the number of passengers through a checkpoint on a given day, the stricter the scenarios seem to be?

Mr. TSAO. Again, sir, the screeners and the screening supervisors are instructed to follow a set of standard operating procedures.

Mr. SMITH. Okay. Thank you, Mr. Chairman.

Chairman WU. I thank the gentleman from Nebraska and recognize the gentlelady from California.

Ms. RICHARDSON. Thank you, Mr. Chairman. To my colleague there from Nebraska, being a graduate of both UCLA and USC, I would say they neither have the coast, football or a basketball team. They need a little help coming from the west side. We are going to get a gingerly game going here.

I have three questions, and if you could be as brief as possible because they are going to call votes in a moment. Dr. Hallowell, in your written testimony, you note that funding for aviation security R&D for explosives detection has not increased in real dollars since 1996. What budget would you have requested, why, and how would you use it?

Dr. HALLOWELL. Yes, ma'am. I think I would have been inclined to ask for budgets that were very similar to what we received in 2004, 2005 timeframe in that there are still daunting R&D issues that we really haven't attacked properly. And here I am thinking screening of cargo which certainly is looming on the horizon and a few other technological breakthroughs that we need to pursue to have some technology enablers to look at other things such as checkpoints that are more user friendly and more integrated and faster as well.

Ms. RICHARDSON. Would you supply this Committee in the future that information?

Dr. HALLOWELL. Yes, ma'am, I will take that for the record.

Ms. RICHARDSON. Okay. Thank you. My second question is what is the status of the frequent traveler program? I heard a little bit about it six months to a year ago where if people who fly on a regular basis, they would get a certain kind of ID card and it was being used, piloted at a few of the locations. What is the status of implementing that program?

Mr. TSAO. Yes, ma'am. I believe you are referring to the registered traveler program?

Ms. RICHARDSON. Yes.

Mr. TSAO. That program is basically a private-sector program. It is run by a coalition of private-sector interests which we interact with. I am not the expert on that program. I can tell you it is out of the pilot stage and it is being broadly used at some of the airports. We have been asked to evaluate some of the technology that they have used, but I am really not qualified to answer any of the programmatic questions.

Ms. RICHARDSON. Okay. Could you supply this Committee with the information——

Mr. TSAO. Yes, ma'am.

Ms. RICHARDSON.—of who is doing the program how the results are?

Mr. TSAO. Yes, ma'am.

Ms. RICHARDSON. And then my third and final question which I think is to you, Mr. Tsao, how many TSA employees would you say, a percentage, are non-U.S. born and how do you recruit?

Mr. TSAO. I am afraid I am going to have to get back to you on both of those questions, ma'am. I don't know specifically any of the statistics.

Ms. RICHARDSON. I realize that the Oklahoma City bombing that occurred was a domestic issue. One of the things I oftentimes get in the airport of people who notice how many people are not U.S.-born who are working as TSA employees. And so I am just curious what the percentage is and what you do to recruit for everyone. So I look forward to that information as well.

Thank you, Mr. Chairman, I hit my deadline in enough time for the gentleman from Nebraska to tease me again.

Chairman WU. We will do a quick round. Those bells, horns, whistles, et cetera, you hear in the background are calling us to votes, and it will be a lengthy series of votes. So it is my intention to permit all Members who wish to do so to ask one further round of questions and then to adjourn the hearing.

And I have only one question, and this is for the entire panel and this is about research priorities. You know, my understanding is that the TSL priorities are set by DHS S&T Directorate which is supposed to look to its customer components, specifically TSA. How do you integrate research priorities from other sources such as the Homeland Security Science and Technology Advisory Committee and industry stakeholders, and also, since IPTs focus on short-term technology development priorities, how do you determine priorities for long-term and more basic research? And I look forward to commentary from folks outside of TSL and TSA also.

Dr. HALLOWELL. Yes, sir. I think right now the research priorities are being driven by the capstone integrated product teams Under Secretary Cohen has set up. He has a number of capstone integrated product teams, certainly the one, government explosives detection, is chaired by Administrator Polly and also has other sitting Members as well. The purpose of that capstone team is to identify gaps that need to be addressed in terms of what the customer needs. It is the role and responsibility of the Science and Technology Directorate to turn those gaps into an idea of what kind of research, enabling research, needs to be conducted to start identifying the R&D needs. So prioritization is made within S&T. The capstone process has just really initiated this year, and I believe it has been fairly successful. The point is the integrated product team is not just a two-year initiative. This was actually driving

R&D that goes out far into the future. Adam, would you like to comment as well?

Mr. TSAO. Yes, sir. I think the community is really starting to come together, and quiet honestly, it has been sparked by Admiral Cohen's institution of IPT's. Last year was the very first year for that, and I think we have learned a lot about who we are and who has expertise within DHS and outside of DHS. And that community is coming together through this process.

Chairman WU. Doctors Oxley or Drury, would either of you care to comment on the setting of priorities and the balance between short-term and long-term research?

Dr. OXLEY. I certainly hope that that is something that we will accomplish in setting up our new center which has been announced but not officially awarded yet. It is something we are having constant discussion on and reaching out to the entire community of folks, not just the university people so that we are in touch with that.

I think to counteract terrorist bombings and IED's, it is going to take a multi-prong approach. It is not simply protection, it is pre-bomb making and it is post-bomb making. So it is hardening. And all of those issues are addressed at various places, and we hope to pull them together.

Dr. DRURY. Purely from a human factors engineering point of view, there has been considerable work done but focused largely on the screening process. There are a lot of other areas where this work needs doing on a more developmental, short-term basis. I think there is a lot more work that needs doing on a long-term basis of how people make decisions under stress effectively and how you can support them in doing that.

Chairman WU. Thank you very much. The gentleman from Nebraska?

Mr. SMITH. Thank you, Mr. Chairman. Mr. Tsao, if you wouldn't mind, how does TSA determine aviation security strategy and equipment requirements? Do you consult with the technical expertise at TSL in order to do so? And furthermore, how does science and technology adjust its R&D efforts to reflect the equipment requirements from TSA?

Mr. TSAO. Thank you, sir. We absolutely discuss—we have a very open dialogue with TSL. Again, we set the requirements. We know what the threat streams are, we know what the vulnerabilities are, we know what our screeners need. We are understanding our passengers I think better than we have in the past. So it is incumbent upon us to set the tone on where research and development, both short-term and long-term, need to go.

As far as how we determine the technologies, often something will come through the door. It looks promising. TSL, will you look at it? Does it do what it say it is going to do? They will test it. Yes, it does what it says it is going to do. Okay. We will look at it. If it can do what it says it can do, how can we use it? All right. Now, this is how we are going to use it. Will using it in this manner meet our operational needs? They will go back and a look and say yes, in this manner it will detect with a certain probability of detection, a certain false alarm. We will go back and then we may—ased on that laboratory results we may start a pilot and it may turn out that in the airport environment, you know, this brand-new widget cannot handle the volume of people we need to put through it. Or in some cases there are a lot of very promising technologies where the timetables are just too long. I mean, we really need to average any process we have. It can't really go beyond 15 or 20 seconds, otherwise you start significantly, you know, jamming up our checkpoints which causes additional security problems.

So there are things that may be useful but they need to get themselves engineered to the point where they meet our operations. If all that occurs and we find something that meets our detection needs, meets our operational needs, we know it is not going to break down. We know that the screeners are going to be able to use it. We deploy that stuff fairly quickly. I think one example you might see, in the work we had done with the lab, is the procurement of the FIDO Paxpoint. This was a piece of equipment that was really in a rack looking for bombs. We were able to modify it to look for the emerging homemade explosive threat. We did that, made a procurement, had it on the street in less than six months. So I mean, we are really trying to be more, I should say, adaptive as the threats come in.

Mr. SMITH. Okay. Thank you. Dr. Hallowell, in your testimony you state that the independent tests and evaluation group and research and development group "set their priorities using different methodologies". How do you see these methodologies varying and how would their priorities compare with those laid out by TSA?

Dr. HALLOWELL. Well, there are two different teams of my people in my laboratory. The independent test and evaluation team really does the kinds of tests and evaluations that directly support activities planned by TSA for piloting or deployment. So that particular team works very, very closely with Mr. Tsao and his group to determining their priorities. And this happens every day. Priorities will change based upon what their interests are and what the threat level is in Intel and things like that. So far we have been actually able to test almost everything I believe he asked us to do and get it done on a fairly timely basis.

The other team, the R&D team, actually is doing different things for a living. They are looking at technology at various technology readiness levels. So it could be like a breadboard or a prototype, and those things typically come out of R&D land, although we do have a pretty active program where we work directly with industry under cooperative research and development agreements to help mature technology.

So if you work for a company, you think you have a solution that can find a bomb, what I say to you is please bring it to my laboratory and let us shake it down. And the way we shake it down is of course we have every flavor explosive and we can evaluate it understanding well what our customer needs are so we can advise companies as to how to grow their technology to get closer to the requirements of the customer.

So that is more of an R&D kind of look-see, how are you doing, what can you do, what can you not do, and what are the opportunities for improvement.

Mr. SMITH. Thank you, Mr. Chairman.

Chairman WU. I thank the gentleman. The gentlelady from California?

Ms. RICHARDSON. Yes, Mr. Tsao, in your testimony you said that talking about the standard and your turning around products, in your testimony you say that TSA develops and identifies the requirements that must be met for procurement to proceed. We have heard from aviation security industry stakeholders, however, that testing new technologies sometimes suffers because new and emerging technologies are tested against old standards of performance. What is TSA doing to update those standards in light of new technologies, and what support does TSL provide to this process? And finally, how do you engage in the private sector when setting performance standards for these newer technologies?

Mr. TSAO. Yes, ma'am. I guess it all goes to what our current capabilities are and what the needs are. If we are talking about a new technology competing with the old technology, that new technology has to do at least what that old technology does. So there is very little we can do about or we would be interested in doing in degredating those standards.

However, if there are situations again where our capabilities are not where they are supposed to be and we see a new technology, we are very flexible in the sense that it gives us a chance. If you have something that gives us a chance, you know, I am not going to hold it to a standard that is not reachable in the short-term. That just doesn't make any sense from a risk standpoint.

Now, we would expect that over time you would be able to get to, you know, develop and again provide more capabilities, but we are in a very adaptive world and I need to be as adaptive as possible.

Dr. HALLOWELL. Yes, ma'am. I would just like to add to that that often TSA does come to us, and they are interested in the technology and they ask us what is the art of the possible? Right now we are involved in doing a market survey and also just evaluating technology for a product line that the CTO is very interested in. So we do an evaluation of what is available and advise them so they have a heads up. It is a little bit more than just detection, but we do look at emerging technology to help TSA.

Chairman WU. I thank the gentlelady, and before we bring the hearing to a close, I want to thank all of our witnesses for testifying before the Committee today. The record will remain open for additional statements from Members and for answers to any follow-up questions that Members of the Committee staff may ask of the witnesses. I thank you all for making the journey for your presence today, and despite whatever our discussions have been through this process, I actually feel better about going to the airport the next time I will be going. Thank you very much for being here today. The hearing is adjourned.

[Whereupon, at 2:10 p.m., the Subcommittee was adjourned.]

Appendix:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Susan Hallowell, Director, Transportation Security Laboratory, Science and Technology Directorate, Department of Homeland Security

Questions submitted by Chairman David Wu

Q1. In your written testimony, you said that funding for aviation security R&D for explosives detection has not increased in real dollars since 1996.

How has the lack of investment affected aviation security generally?

A1. Aviation security is continually improving with the introduction of new homeland security technologies. For example, in April, the Department announced checkpoint technology improvements that will further strengthen aviation security while decreasing the hassle factor for travelers. The S&T Directorate's work in transportation security R&D will lead to the next generation of passenger screening. This includes stand-off detection of explosives, detecting suicide bombers, improving the capabilities of canine explosives detection teams and creating the next-generation passenger checkpoint. Investment in this and other aviation security R&D is based on priorities identified by the Transportation Security Administration (TSA) and the Administration, as supported by Congress.

Performers carrying out aviation security R&D include the S&T Directorate's Transportation Security Laboratory (TSL) as well as universities, national laboratories and industry.

Q2. What projects have been delayed or canceled because of a lack of funding?

A2. The S&T Directorate's investment in R&D related to aviation security includes a broad range of activities across the S&T Directorate. Several projects address priorities identified by TSA through the S&T Directorate's capstone Integrated Product Team (IPT) process. Those priorities include:

- Technologies to screen people for explosives and weapons at fixed aviation and mass transit checkpoints—In particular, to allow higher detection rates with minimal disruption to passenger flow;
- System solutions for explosives detection in checked and carried bags—In particular, automated systems to screen for conventional explosives, liquids, weapons, and homemade explosives;
- Capability to detect homemade or novel explosives—In particular, characterizing potential homemade explosives for use in developing detection systems for screening at checkpoints;
- Optimized canine explosive detection capability—In particular, techniques, training tools, and methods to improve performance for all transportation venues; and
- Technologies for screening air cargo for explosives and explosive devices—In particular, technologies for screening break-bulk, palletized, and containerized air cargo.

Lower priority project areas that are not funded or have reduced funding include: (a) development of containerized and palletized cargo inspection technologies, (b) shoe scanner technology development, (c) advanced explosives detection systems for checkpoints and checked baggage, (d) enhancing trace "puffer" portals, and (e) developing integrated checkpoint systems.

Q3. How will the continually decreasing investments affect aviation security as a whole over the next five to ten years?

A3. The investment in aviation security technology is not "continually decreasing." There are numerous projects across the S&T Directorate that will help ensure the safety of passengers throughout the transportation sector. The S&T Directorate's investment in aviation security R&D spans basic research to technology transition to customers in a number of areas, including hostile intent, transportation security and countering improvised explosives devices. Investment which explicitly applies to detecting and mitigating explosives on aircraft was $23.5 million in FY 2007 and $25.3 million in FY 2008. The President's FY 2009 budget request of $42.3 million nearly doubles that amount. The S&T Directorate plans to continue significant investment in aviation security R&D in the out years.

Q4. You noted that TSA is responsible for setting performance requirements for technology.

Has TSA done an acceptable job at sharing their performance requirements for new technology in a timely and useful manner?

A4. The process for receiving requirements from the Transportation Security Administration (TSA) has improved with the implementation of the S&T Directorate's Integrated Product Team (IPT) process. Through this process the S&T Directorate receives requirements from TSA and designs programs that will develop products to meet these requirements. In addition, there is frequent and open discussion between the S&T Directorate and TSA on the development of certification and qualification requirements for specific products.

Q5. What improvements are necessary in the communication between TSA and TSL?

A5. The S&T Directorate's capstone IPT process brings leadership and staff from TSA and TSL together to discuss research and development priorities and plans. While the IPT process has improved communication, security requirements for the Transportation Security Administration (TSA) can change rapidly given the adaptation of terrorist techniques. This makes having numerous and open lines of communication vital. Examples of ongoing efforts to improve communication with TSA include:

- The S&T Directorate has detailed several of its Transportation Security Laboratory (TSL) staff to TSA. A test engineer was detailed to TSA's Network Management group to support cargo projects and a Human Factors subject matter expert is about to begin a detail to TSA headquarters. This should facilitate open and frequent dialogue about TSA requirements with TSL R&D personnel knowledgeable in the science of detection and deterrence.
- The S&T Directorate and TSA are looking for ways to exchange expertise to provide input on available technology opportunities. The S&T Directorate's R&D scientists at TSL recently investigated millimeter wave technology, and are providing an overview of the technology's capabilities to TSA.
- The S&T Directorate plans to schedule more frequent program and technical reviews between TSA and TSL, which should contribute to collateral pursuit of optimal security solutions.

Q6. You describe the Transportation Security Laboratory as "committed to providing technical and procedural solutions that work in the field." Yet TSL does not carry out field testing of technology.

How does TSL gather information on technology successes and failures after those technologies are deployed?

A6. The Independent Test and Evaluation (IT&E) group at the Transportation Security Laboratory (TSL) receives information on post-deployment performance through regular briefings from teams conducting field performance verification testing for the Transportation Security Administration (TSA), as well as during S&T Directorate Integrated Product Team (IPT) project-level IPT meetings, where deployment issues are routinely discussed.

Q7. What steps does TSL take to improve technologies after problems are identified, and how do you test whether those problems are indeed solved?

A7. When issues arise in the field, TSA notifies the lab and TSL works with the vendors to address problems. This often includes review of the vendor's Engineering Change Proposal (ECP) to, in part; determine if additional testing is required to validate the solution. In addition, TSL maintains an operational version of a given product, and pursues diagnoses of field issues by trying to replicate problems on these maximally performing systems. When new threats are identified, as with the homemade explosives threat, TSL works closely with TSA to identify capability gaps and pursue solutions with industry and international partners.

Q8. In your testimony, you argue that the Transportation Security Laboratory should be allowed to charge companies for certification of their products.

If TSL was authorized to charge for certification services, how much additional lab capacity and how many additional employees would need to be created in order to offer this service, especially given TSL's increasing workload from TSA?

A8. If the Transportation Security Laboratory (TSL) was authorized to charge for certification services, TSL would need to increase laboratory capacity and employees over the next several years as follows:

a) Administration of Customer Charging. TSL estimates this would require additional personnel to perform financial management, financial analysis, customer coordination and scheduling services.

b) Infrastructure Investment. In order to accommodate the increasing need for services, TSL would need to add (i) an Explosive Storage Facility, (ii) an Independent Test and Evaluation (IT&E) Facility, (iii) a Test Article Storage (non-explosive) Facility and, (iv)Expanded Office Space.

c) Personnel. TSL would need to add eight additional personnel to meet the added workload, including four general/system engineers, one mathematician, one explosives specialist and two explosives handlers.

d) Operations and Maintenance. TSL would require additional Operations and Maintenance investment to support the new facilities and added workload.

These investments would enable TSL to fulfill the inherently governmental function of maturing and certifying technology and expand testing and development to additional customers.

Q9. How would TSL determine which products to accept for certification, and how would you set performance requirements?

A9. The S&T Directorate's Transportation Security Laboratory (TSL) performs certification at the request of the Transportation Security Administration (TSA), using performance requirements set by TSA. As DHS develops standards for other DHS applications (beyond transportation security), the S&T Directorate plans to certify equipment for other applications. Vendor products that have achieved a sufficient degree of technical readiness would be accepted on a first-come, first-served basis, provided TSL has sufficient capacity to take on work beyond its DHS directed workload.

Q10. Would all companies be charged for testing services, or only those that approached TSL without a request from TSA?

A10. TSL does not plan to charge companies that are responding to a request from TSA. TSL would charge companies that approached TSL without a request from TSA. These may include, for example, international technology developers.

Questions submitted by Representative Phil Gingrey

Q1. Frequent travelers are continuing to enroll into the Clear Traveler Program that allows them to navigate security lines at airports more expeditiously. While Clear is one example of how a private company can work to both keep us safe and move us through the security screening process in a speedy manner, to what extent does the Federal Government partner with companies such as this to stay on the cutting edge of security screening and airport safety?

Furthermore, since this is the general direction that we are moving for aviation security, what potential challenges will we face in terms of public/private partnerships in this realm, the storage of biometric information, and the continued advancement in aviation security technologies?

A1. In support of a formal, systematic approach for coordinating with stakeholders and facilitating an effective and efficient exchange of information regarding Transportation Security Administration (TSA) requirements and future deployments of screening technology, the Industry Outreach group within the TSA Office of Security Technology (OST) was created to formalize the communication mechanisms by which OST, customers, and security partners exchange ideas, information, and operational expertise. Collaboration on the technology security requirements and deployment strategies leads to the successful deployment of cutting-edge, state-of-the-art technology solutions.

In order to ensure that the TSA is increasing its efforts to strengthen the relationship with security partners, Industry Outreach regularly participates on industry and association-sponsored panels to discuss technologies available for passenger, baggage, and cargo screening. Currently, Industry Outreach is in the process of organizing industry roundtables where security partners will be afforded a better understanding of TSA's vision for future technologies. Industry representatives will also be asked to provide the OST with feedback regarding their concerns. OST understands the importance of receiving industry feedback and to that end the "Planning Guidelines and Design Standards for Checked Baggage Inspection Systems," distributed in October 2007, now has an e-mail address where our industry security partners can submit comments for consideration in the next version of the guidelines. The OST Industry Outreach also participates with the Office of Commercial Airports in TSA's Office of Transportation Sector Network Management on a regular basis. Individual airports are encouraged to contact OST Industry Outreach with any airport specific concerns they may have. In addition, Industry Outreach also regularly conducts site visits and attends conferences. Industry Outreach is also supporting a new planning process for airports to apply for fiscal year (FY) 2009 and FY 2010 funding for electronic baggage screening systems.

As mentioned above, on September 11, 2007, TSA issued the "Biometrics for Access Control Qualified Products List." This document is an excellent example of how TSA is working with industry to stay on the cutting edge of biometric technology. This qualified products list (QPL) is intended to identify biometrics devices for access control systems which have been tested and found to be in compliance with performance specifications as set forth in the Guidance Package Biometrics for Access Control published on September 30, 2005. The testing/qualifying process is a continuous, open, and ongoing activity and is not intended to endorse one product over a competitor's product, and the TSA does not recommend one over another. The QPL is established merely to provide information to airport operators on products that have been tested and meet TSA standards, for their use in conducting source selections and procurement actions, if needed. Users are cautioned to only rely on the presence of a product on this list as one important but not comprehensive piece of information in an overall airport biometric acquisition and deployment decision.

OST is currently working with the National Institute of Standards and Technology (NIST) to establish a process to qualify biometric testing facilities to further update this QPL (Transition Phase), while also working with NIST and other organizations within the Department of Homeland Security, to develop an agency-wide biometrics testing lab accreditation process. Once that process is established, testing labs must obtain NIST Accreditation (NVLAP) in order to test devices for inclusion on the QPL. Manufacturers may submit their devices to a NVLAP accredited lab of their choice and the lab will submit test results to TSA for analysis and inclusion on the QPL.

All manufacturers/vendors of biometrics for access control systems may participate in planned future testing and the QPL will be periodically updated to include new information about existing products and additional products that qualify. Government and industry working together will ensure that the biometric systems are effective, reliable, and secure.

The potential challenges in the storage of biometric information include privacy protection, records retention, and the systems required to house the data. However, only minimal data is stored on the Registered Traveler (RT) card. The card contains only enough biometric data, stored within an applet on the card, to confirm a person's identity when he or she travels. As a safeguard against biometric theft, fingerprints are not stored on the RT card as an image, but as biometric template data which prevents unauthorized parties from replicating the fingerprint image.

TSA will continue to look toward partnership opportunities to assist in expediting the security process.

Q2. How should TSA determine the appropriate mix of technology and people in its aviation security and other modes of transportation?

A2. The Transportation Security Administration (TSA) constantly advances its technology usage to stay ahead of emerging threats. We know there's no single silver bullet technology, no game-changing technology that will, at once, take us back to pre-9/11 convenience. But by upgrading what we do have—our workforce and technology resources—and combining this with the other layers of security and process innovation, we can get the security result we need, with a lot less hassle for passengers.

TSA's layered approach to security seeks to identify and deter threats well before they reach the Nation's airports, railways, highways, mass transit, ports and pipelines. This risk-based security strategy relies on transportation-specific intelligence, so TSA coordinates closely and shares information with other Department of Homeland Security (DHS) components, the intelligence and law enforcement communities, other government departments and agencies such as the Department of Transportation and the Federal Aviation Administration, and the transportation industry. Transportation-specific intelligence is critical to TSA's overall risk-based security strategy, and the products of such intelligence provide a threat framework to prioritize limited security resources.

TSA reviewed all modes of transportation and set risk-based priorities. These priorities focus TSA's attention and limited resources—both people and technology—on the most critical issues. TSA has conducted or participated in various risk analyses that compare risks across different transportation modes, including the DHS

Strategic Homeland Infrastructure Risk Assessment. Surface transportation, transit, and rail are, like aviation, high priorities for TSA. The level of funding is determined by the degree to which TSA can effectively mitigate the risks, compared to the degree with which industry and other stakeholders can mitigate the risks.

TSA takes a network approach to transportation security and views it as a shared responsibility and effort among all of TSA; the Department of Homeland Security (DHS); other government agencies and entities at all levels, including federal, State, local, tribal and territorial; and owner-operators.

Much of the Nation's aviation infrastructure is federally owned. Surface modes of transportation are approximately 95 percent privately owned and operated. They receive security funding support from multiple streams (i.e., State, local, private, as well as federal). The Department has consistently stated that responsibility for surface transportation security is a shared responsibility among a variety of stakeholders, including State, local, and federal agencies, and private owners and operators. The appropriate role for the Federal Government includes: using the substantial resources already in place and providing critical information; setting national priorities; developing transportation security fundamentals; coordinating ongoing efforts; and encouraging certain actions that reduce risk to the Nation's transportation system.

The bulk of federal spending in aviation security has covered the compensation and benefits of Transportation Security Officers, who work every day in more than 450 airports nationwide to ensure the skies remain secure. Aviation security allows for point defense. We can seal off an area of the airport and only permit entry to those with tickets who have passed through screening.

The rail and mass transit modes do not accommodate this type of approach. These systems operate over a broad geographic spread with numerous stations and transfer points providing the efficiency and fast-pace that are essential to moving thousands of passengers, particularly during daily rush hours. The point defense approach taken at the airports is neither practicable nor desirable. Rather, an integrated strategy, tapping the strengths of the Federal Government, State and local governments, and passenger rail and mass transit agencies, must be pursued.

In evaluating the resources required to address surface transportation risk issues, it is important to account not just for TSA's budget and statutory obligations in aviation, but also the substantial efforts, capabilities and expertise that already exist in the surface transportation environment, as well as very different operating, legal, and resource requirements. Therefore, the level of TSA's budget allocated to surface transportation security relative to aviation only partially reflects the overall relative risk between them. In fact, TSA does give attention and priority to surface transportation, but TSA's role relative to the security partners in the networked approach is different than it is in aviation.

The appropriate way, therefore, to determine the appropriate mix of technology and people in aviation security and other modes of transportation, is to use the same criteria that we use to evaluate all proposed security measures. These criteria are based on risk management (how substantial is the risk that the measures addresses and how much does it mitigate the risk), layers of security (how does the measure complement and enhance other existing security measures) and the needs and constraints posed by any given mode of transportation where the measure might be applied.

Q3. Please respond to the three questions below:

What is the technical background of employees working at TSL?

A3. The S&T Directorate's Transportation Security Laboratory (TSL) federal staff is composed of scientists (physicists, chemists, research psychologists and mathematicians) and engineers (aerospace, mechanical, chemical and electrical), certified project managers, explosive handler specialists, safety and security specialists and administrative personnel.

Q4. How many of your employees have science or engineering degrees?

A4. Twenty three percent of TSL staff members have obtained doctorate degrees, mostly in science and some in engineering, 38 percent of the staff hold Master's degrees in science or engineering and 11 percent of the staff holds Bachelor's degrees, predominately in science and engineering. The rest of the staff has Associate's degrees in a variety of areas. About 70 percent of the staff performs technical roles, while the remainder perform program management, administrative or safety and security functions. Of the technical staff, about half support research and development (R&D) activities and half support test and evaluation activities for the Integration, Test and Evaluation (IT&E) and R&D groups.

The TSL federal staff is supplemented by an equivalent number of contractors as well. Their technical background and distribution of labor functions are similar to the distribution of the federal staff.

Q5. Can TSL recruit qualified scientists to perform testing and evaluation without also providing for opportunities to perform basic and applied research?

A5. The S&T Directorate successfully recruits highly qualified test engineers as well as scientists to work at the Transportation Security Laboratory (TSL). Highly qualified professionals are attracted by the range of work conducted at TSL, which involves basic and applied research in the development of new standards and technologies. Many of these professionals are also attracted by TSL's rich history of successful product development and technology life cycle management as well as the international recognition TSL has received for its role in the development of standards, protocols and test articles necessary for detection technology assessments. However, due to the length of time it takes to hire, we do loose recruits to other jobs.

Q6. Your testimony describes how TSL uses core funding to respond to unforeseen requests for scientific and technical advice.

How much of your budget has gone to these activities over the last five years?

A6. It is estimated that about 25 percent of the Transportation Security Laboratory's (TSL's) budget has been used to meet unforeseen, rapid response requests from TSA and other customers. These requests have included rapid turnaround analyses of developing or deployed technologies, requests for advice on technology suitability, and requests for analysis in support of TSA's project-level Integrated Product Teams (for cargo, checked bag and checkpoint technologies).

Q7. Do you believe TSL is prepared to quickly respond to similar requests in the future?

A7. Yes.

Questions submitted by Representative Laura Richardson

Q1. In your written testimony you note that funding for aviation security R&D for explosives detection has not increased in real dollars since 1996.

What budget have you requested and how would you use it?

A1. Aviation security is continually improving with the introduction of new homeland security technologies. For example, in April, the Department announced checkpoint technology improvements that will further strengthen aviation security while decreasing the hassle factor for travelers. The S&T Directorate's work in transportation security R&D will lead to the next generation of passenger screening. This includes stand-off detection of explosives, detecting suicide bombers, improving the capabilities of canine explosives detection teams and creating the next-generation passenger checkpoint. Investment in this and other aviation security R&D is based on priorities identified by the Transportation Security Administration (TSA) and the Administration, as supported by Congress.

Performers carrying out aviation security R&D include the S&T Directorate's Transportation Security Laboratory (TSL) as well as universities, national laboratories and industry.

The S&T Directorate's FY 2009 budget request for Laboratory Facilities funding in support of the Transportation Security Laboratory (TSL) is $21.55 million. This would fund TSL operations, maintenance, employee salaries and expenses. In addition, the S&T Directorate's budget request includes program funding that would fund activities at TSL. A significant portion of this investment would come from the S&T Directorate Explosives Division's FY 2009 budget request of $96.15 million to fund the following programs. TSL will be one of the performers carrying out this work.

- Homemade Explosives (HMEs) Program—Investigates all potential detection technologies capable of detecting and distinguishing explosives and flammable liquids from benign liquids (e.g., drinks, hygiene products and contact lens solutions).
- Cargo Program—Develops advanced air-cargo screening systems and improves canine detection capabilities.
- Check Point Program—Develops advanced capabilities to detect explosives and concealed weapons, including small Improvised Explosives Devices

(IEDs) or HMEs, which terrorists could use in the hostile takeover of mass transit.

- Manhattan II Program—Initiates cost performance tradeoff studies to provide TSA better information upon which to acquire the "best performance and affordability" screening systems.
- Conveyance Protection Program—Assesses risks and mitigates consequences of intentional assault on air, surface and marine vehicles.
- Explosives Research Program—Improves explosives detection capabilities by performing multi-disciplinary research and development in imaging, particle physics, chemistry, and algorithms. These result in the development of enhanced detection capabilities and lead to next-generation detection systems.
- Deter Program—Conducts social and behavioral sciences research to identify actionable indicators and warnings of IED threats posed by individuals and groups in the United States.
- Predict Program—Develops technologies to secure U.S. borders that will automatically identify, alert on, and track suspicious behaviors that precede a suicide bombing attack; and automatically identify and prioritize the risk of likely potential targets of attack.
- Detect Program—Develops advanced technologies to detect explosive threats to the Nation's aviation, rail and ship transportation systems.
- Respond/Defeat Program—Conducts R&D to better respond to and defeat explosive threats.
- Mitigation Program—Reduces the effects of bombs that cannot be detected or cannot be rendered safe through practical and available means.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Adam Tsao, Chief of Staff, Office of Operational Process and Technology, Transportation Security Administration, Department of Homeland Security

Questions submitted by Chairman David Wu

Q1. How does TSA define field testing protocols? In what ways do field tests differ from lab tests and certification procedures, and how are the results reported to TSL?

A1. Independent operational (or "field") testing and evaluation (OT&E) is the means by which the Transportation Security Administration's (TSA) Office of Security Technology (OST) characterizes the operational effectiveness and suitability of viable security technologies and systems in the field environment. Operational testing uses typically-trained operators and maintainers, operating production-representative systems, in accordance with the approved concept of operations within the intended operational environment.

Operational testing primarily differs from laboratory or certification technical testing in the degree of operational realism afforded by testing within the intended environment. In addition, OT&E supports increased focus on suitability evaluation areas (including operational reliability and maintainability, logistics supportability, manpower and personnel requirements, training, and human factors engineering) through use by the intended target audience and with the intended support concept. As such, OT&E results present the most realistic portrayal of anticipated system performance within the field environment.

The Department of Homeland Security Transportation Security Laboratory (TSL) provides TSA with results of their laboratory testing through classified briefings and formal reports. TSA operational field tests are conducted subsequent to laboratory testing. The results of field testing are for TSA use and it is not a requirement to provide operational test reports to TSL. Although results are not formally reported back to the TSL, the TSL does provide representatives to TSA project specific Integrated Product Teams. All program aspects, including operational test results, are discussed in this forum.

Q2. According to Dr. Hallowell, the Transportation Security Laboratory has formal procedures in place to ensure that they are responding directly to TSA's research, development, testing, and evaluation needs. How successful has TSL been at meeting TSA's needs? Does the Integrated Product Team process capture adequate information about TSA's capability gaps and research priorities? Are there any changes to this process that you would recommend?

A2. The Integrated Product Team (IPT) process is in its initial stages, having just been included in Transportation Security Administration's (TSA) fiscal year (FY) 2009 budget. The IPT has been organized into 13 capstones programs, to complement the research and development efforts of TSA. The Explosives Detection Division Capstone IPT was created during the current FY 2009 budget cycle.

This initial pilot program was successful in many of its goals, including establishing budgetary funding priorities as part of the FY 2009 budget process and in prioritizing the research and development needs of TSA. As of November 2007, the Explosives Detection Division Capstone IPT has shown that TSA is able to articulate to the Department of Homeland Security Office of Science and Technology a clear understanding of its science and technology needs to procure solutions that not only meet stringent detection thresholds, but also meet throughput requirements in support of the aviation sector.

Currently, a more in-depth report card of the IPT Process is premature at this time, as the program is still too new. As already stated, the goal of the IPT Process is to address and reach a better understanding of the operational needs of TSA and to ensure the research and development efforts of TSA are timely and relevant. Initial feedback on the initial capstone program has been very promising.

Q3. How often does TSA turn to the Department of Energy's National Labs or private labs to carry out testing that could be performed by the Transportation Security Laboratory? In those instances, why does TSA choose to use resources other than TSL, and what is the added cost to TSA?

A3. The Transportation Security Administration (TSA) actively pursues a number of options to readily interject new screening technology into the operating environment. TSA coordinates with the Department of Homeland Security's Science and

Technology Directorate (S&T) to determine the most efficient way to achieve that goal. In general, TSA and DHS choose to use the National Labs when the opportunity is available to leverage existing expertise that has been developed for other government programs. It would be cost prohibitive for S&T to develop similar in house capability and expertise.

Q4. In her testimony, Dr. Hallowell says that "it is the responsibility of TSA to define and judge readiness for deployment." How does TSA determine whether a technology is ready for deployment? If technologies are deployed in spite of expressed reservations from TSL, what steps are taken to ensure that those technologies meet performance and technical requirements?

A4. The Transportation Security Administration (TSA) considers evaluation products from a variety of sources (including the Department of Homeland Security Transportation Security Laboratory (TSL) and other technical testing data sources, such as independently validated vendor information) in considering readiness for deployment of security systems and technologies. In addition to reviewing the demonstrated effectiveness and suitability of candidate systems (as evaluated against Operational Requirements Documents, procurement specifications, and other applicable statutory and regulatory requirements) as noted during both developmental and operational testing, the TSA Office of Security Technology also considers the operational capabilities afforded by the system of interest, as well as resource requirements, operational need, and threat information, among others, in determining how and whether a system should be deployed.

Q5. How are human factors taken into account when developing functional requirements for new technologies? In what ways do requirements take both screener and passenger needs into account?

A5. Human Factors Engineers participate at every stage of the requirements development process and in system reviews. They ensure that requirements for human interfaces effectively address usability and ergonomic aspects. These requirements are written to ensure that screening equipment is user friendly so that operators can work efficiently and safely and passengers will be able to submit to screening in ways that are safe and minimize stress. The Transportation Security Administration (TSA) and the Department of Homeland Security's Science and Technology Directorate work together to provide human factors input into requirements development, system and critical design reviews, and system qualification. TSA then evaluates Human Systems Integration when systems are piloted in the field.

Q6. Dr. Drury's written testimony describes the Threat Image Projection System (TIPS) as one example of how human factors research can positively affect the efficacy and speed of aviation checkpoints. TIPS enhances screener performance by randomly inserting threat images to ensure that screeners are regularly presented with potential threats and can react accordingly. Does TSA plan to include a system like TIPS in airports?

A6. Threat Image Projection (TIP) is currently active on over 1,800 TIP Ready X-ray (TRX) machines at all passenger screening locations nationwide. TIP provides screeners experience in identifying threat objects including improvised explosive devices, guns, knives, and other deadly and dangerous prohibited items (i.e., martial arts weapons, tools, and brass knuckles, among others). The TIP library contains over 2,400 fictional threat images captured at various angles and difficulty levels. TIP serves as an invaluable, multi-functional system that extends well beyond an evaluation tool; it provides immediate feedback and functions as a reinforcement system that increases screener accuracy. TIP enhances screener attentiveness and vigilance through random and periodic presentations and exposure to new and emerging threats. TIP results, which have been collected and analyzed on a monthly basis since January 2004, have shown a steady increase in screener performance on threat detection. These results are used to track trends in screener performance on threat detection, as well as identify additional training needs.

Q7. What is the technical background of employees working at TSA? How many of your employees have science or engineering degrees? How has TSA staffed its teams responsible for developing functional requirements for new technologies with respect to R&D expertise?

A7. Overall, the Transportation Security Administration (TSA) tracks the education level completed, such as Associate degrees, Master's degree, and so on. We do not capture the course of study; that is, Engineering vs. English, mathematics or biology. Attached is the information available about degrees.

Description	# of Employees
Associate degree. 2-year college degree program completed	1804
Bachelor's degree. Requires completion of at least four, but not more than 5, years of academic work; includes Bachelor's degree conferred in a cooperative plan or program that provides for alternate class attendance and employment in business and industry.	4646
Master's degree. For liberal arts and sciences customarily granted upon successful completion of one (sometimes two) academic years beyond the Bachelor's degree. In professional fields, an advanced degree beyond the first professional but below the Ph.D.	942
Doctoral degree. Includes such degrees as Doctor of Education, Doctor of Juridical Science, Doctor of Public Health, and the Ph.D. (or equivalent) in any field. Does not include a Medical Doctorate.	57
Total	**7449**

TSA's Office of Security Technology (OST), which is primarily responsible for developing functional requirements for new technology, has 77 employees on board. Of that number, approximately 40 employees have science or engineering degrees, many with advanced graduate degrees and a few with Doctorate level degrees. The OST staff includes a Chief Scientist and Chief Engineer, adequately addressing the need for research and development expertise and the functional requirements for new and emerging technologies. OST continues to hire in the science/engineering fields.

Question submitted by Representative Phil Gingrey

Q1. Your testimony states that "TSA's involvement will likely vary" in future technology development and implementation. What factors would lead to decreased involvement by TSA in any particular aviation security project?

A1. The statement about the Transportation Security Administration's (TSA) involvement in future technology development does not mean that TSA envisions decreased participation in future efforts. Based on the maturity of screening technology at the time of assessment as well as the operational rigor required for implementation and integration, the project areas of responsibility are shared but will vary between TSA and the rest of the Department of Homeland Security.

Questions submitted by Representative Laura Richardson

Q1. What is the status of the Registered Traveler (RT) Program?

A1. The current phase of the Registered Traveler (RT) Program is known as the Registered Traveler Inter-operability Pilot (RTIP). The RTIP is entirely fee-funded and intended to test inter-operability between multiple RT Service Providers. A Service Provider (SP) is a private sector vendor chosen by a Sponsoring Entity to implement RT as its agent. As of May 2008, 19 Sponsoring Entities, participating airport authorities or air carrier operators, are operating RT at 18 airport locations, three Transportation Security Administration approved SPs are hosting operational RT Programs, and approximately 110,000 participants are active in the RT Program.

Q2. How many TSA Employees are not US Citizens? How do you recruit TSA Employees?

A2. Currently, all Transportation Security Administration (TSA) employees are United States citizens.

TSA participates in various recruitment activities to enhance awareness of opportunities for employment with TSA and maximize the number of highly qualified candidates for consideration. Recruitment efforts include posting job vacancies on USAJobs, web boards, college campuses, and in various print media. TSA recruiters participate in career fairs and conferences nationwide; establish relationships with community-based organizations, educational institutions, military associations, and cultural organizations. TSA recruiters also participate and attend professional association conferences to network with colleagues, business leaders and individuals in the field who may be resources for identifying qualified candidates. TSA also participates in Department of Homeland Security corporate recruiting events and job fairs, including Veterans Outreach efforts.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Jimmie C. Oxley, Professor of Chemistry, University of Rhode Island (URI); Co-Director, URI Forensic Science Partnership; Co-Director, DHS University Center of Excellence in Explosive Detection, Mitigation, and Response

Questions submitted by Chairman David Wu

Q1. You noted in your testimony that operational difficulties undermine the performance of explosives-detection technologies currently in use in the field. Do existing tests and evaluations of explosives detectors adequately predict these field performance challenges? If not, what additional tests should detectors be subject to in order to ensure high quality performance and robustness?

A1. It is a general phenomenon that lab-scale results will not be directly applicable to real-world scenarios. Therefore, there is an intermediate step—the pilot-scale. In airport security, the pilot-scale is use of a new device or protocol at a few select airports (test-beds) under carefully controlled conditions. Still, the final performance will also be affected by repetitive use and by incorporation of "lessons-learned" improvements. These steps cannot be avoided. The only way to speed this process is by use of more test-bed facilities. The obvious lack in present technologies is the need to include ergonomic considerations at an early point in instrument design.

Question submitted by Representative Phil Gingrey

Q1. How should TSA determine the appropriate mix of technology and people in its aviation security and other modes of transportation?

A1. It is important to continue vigorous funding for developing and improving technologies—old and new. However, ergonomic factors should be considered early in the development. Presently, people are used in security screening at points where instruments fail. It would be better to assign assets keeping in mind that people are better at decision-making and instruments are better at screening. The only way to get the right balance is to continue and expand use of test-bed arenas.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Colin G. Drury, Distinguished Professor and Chair, Department of Industrial and Systems Engineering, State University of New York at Buffalo

Overall Response: These are excellent and thought-provoking questions that will help advance the cause of improved security, and particularly the role of Human Factors Engineering in helping assure that improvement. I thank the Chairman and Ranking Member for the chance to respond.

Questions submitted by Chairman David Wu

Q1. In your opinion, is there adequate awareness of the need for human factors engineering in the private aviation security technology industry? If not, how should the Transportation Security Administration change their performance requirements to compel companies to consider human factors when designing technology?

A1. There was much talk in security about Human Factors since before TSA was formed, but the term tended to be used rather loosely in the aviation security technology industry. It often meant "training" or "human resources" or "computer screen design." This has improved over the years, so that the equipment manufacturers I have met have a more realistic view of human factors as an engineering discipline. I am still not convinced that they see it as a systems engineering discipline, with all that implies about designing from the start for the human operators rather than meeting a set of fixed requirements.

To "compel companies to consider human factors when designing technology" it would be useful for the TSA to set requirements for the design process as well as requirements for the finished product. These could include employing at least one Human Factors Engineer and ensuring that the process of design was documented to show how that design input was used. Currently full membership in the Human Factors and Ergonomics Society in the USA would ensure adequate technical competence in Human Factors Engineering, but full certification by the Board of Certification in Professional Ergonomics (BCPE) would represent proven expertise in practice of the Human Factors Ergonomics discipline. The design process for the variety of different security systems is unlikely to benefit from rigid requirements. It would be preferable to have a process that called for the manufacturer to use good Human Factors Engineering practices in the design and demonstrate this to competent Human Factors Engineers in DHS (e.g., DHS's Science and Technology or TSL's human factors personnel). Of course, the government Human Factors Engineers would need to demonstrate the same level of credentials called for above.

Q2. You mentioned in your testimony that technology can be tested for human factors by either analyzing the final product or carrying out field testing. Are there options for carrying out performance tests in the lab that would reveal any human-technology interaction problems?

A2. In my written testimony I mentioned both of these as valid evaluation methods. Analyzing the final product for compliance with Human Factors Engineering guidelines may not be as successful because, as noted in the testimony, security technologies are complex and varied so that no single checklist could hope to ensure a well human-engineered system. The field testing alternative favored in the testimony could encompass a range of testing from breadboard testing of early prototypes in a laboratory through to in-service trials at airports or other points of entry. Product and system testing has a long history in Human Factors Engineering, and all levels have been used at different times on many systems. We now have excellent software for simulating working systems using computer workstations so that more realistic tests can be applied at an early stage of systems development. For example, with X-ray screening of carry-on baggage it is quite possible to test new technology and algorithms for detection of threats prior to the technology actually being available for in-service use. In this way we can test, for example, increased system resolution (as was done at TSL) to determine whether or not increased resolution will make any practical difference to threat detection performance.

In all off-line testing it is easier to detect problems than to assure future performance. If the simulated system works well under test conditions, then it may still have undiscovered problems in the field (e.g., maintenance errors), whereas if problems are found during testing they almost certainly would occur in field conditions. Where the test is sited, laboratory vs. field, may be less important than the psychological and biomechanical fidelity of the simulation in predicting future in-service performance. The choice of participants, for example, is crucial. Using personnel from the development team introduces a bias as they both know too much about the new system and have poor current experience of the in-service situation. Similarly using a subject pool of university students may answer some questions (e.g., how well do novices perform under different display options) but is unlikely to yield valid predictions of in-service performance. The measures in off-line testing are also important. As noted in my written testimony, we can take measures beyond performance (hits, false alarms and throughput) under test conditions. We can be prepared to observe human-system interaction errors and interview experienced users after the test to help determine not just that a problem exists but why it exists and how to prevent it. Because off-line testing is controlled, we can use a broad range of threat types and methods of concealment to determine in advance of service use where difficulties are possible, and where the greatest strengths of the new system lie. The textbook *Evaluation of Human Work* by J.R. Wilson and E.N. Corlett (3rd Edition, 2005) has chapters on many of the issues of human factors testing from simulator fidelity to experimental design.

Questions submitted by Representative Phil Gingrey

Q1. Your written testimony describes the Threat Image Projection System (TIPS) as one example of how human factors research can positively affect the efficacy and speed of aviation checkpoints. Can you tell us a bit more about that program including where it was developed and at what cost?

A1. This is a question for which I do not have complete data, so I would refer you to TSL for full information on who exactly developed TIPS and what it cost. I would expect that Dr. Hallowell would be able to make this information available. TIPS was developed at the TSL and won the team the FAA's Distinguished Achievement in Technology Transfer Award. The idea behind TIPS is that it provides realistic test images of threats to the screener during actual operations. These threats images are superimposed almost seamlessly onto items (carry-on bags etc.) that are actually passing through the X-ray scanner at the time and so the threats appear to be items within the bag. The screener presses one of two buttons to release the bag: OK if no threat is seen and Not OK if a threat is seen. If there was a TIPS threat projected onto the bag, the screener gets a response to the effect that they missed a threat (if they indicated OK) or a congratulation on correctly detecting a threat (if they indicated Not OK). When they correctly detect a threat they are instructed to re-inspect the bag in case it also contains an actual threat. The data on hits and misses of TIPS images is collected automatically on most newer X-ray equipment and is downloaded periodically for analysis.

There are five main advantages of the TIPS system:

A. Because of the very low rate of actual threats, TIPS images provide a means of increasing the effective rate of threats in a realistic manner. The higher the effective threat rate, the better the performance in almost any inspection task.

B. This increase in effective threat rate also tends to reduce any time-on-task decrease in performance due to fatigue (the *Vigilance Decrement*).

C. The rapid feedback of success / failure data to the screener also reduces any vigilance decrement. True feedback is problematical in any inspection task, as we almost never know the true presence of a threat. If we did know that, there would be no need for the inspection! Thus the artificial (but realistic) feedback provided by TIPS overcomes a longstanding problem in maintaining inspection performance.

D. Data can be collected on individual screeners, whole screening lines, complete checkpoints and even whole airports for monitoring purposes. In any inspection task, the system will make errors and that is true of automated, manual and hybrid inspection tasks. Collecting the TIPS data on errors permits analysis of differences between screeners, checkpoints etc. and so can point up instances of both high performance and low performance. Action can then be taken to reward or retrain individual screeners, or seek to replicate good screening lines or checkpoints.

E. Finally, the database generated by TIPS can be used to answer many research questions. For example, if threat detection does indeed decrease with time on task (vigilance decrement) the magnitude of the effect should be measurable in TIPS data. It should also be possible to test time-of-day effects, effects of growing screener expertise, the effectiveness of changes to X-ray set-up or procedures, etc.

Note however that for any of these to occur, the TIPS data must be valid. Thus the TIPS library of images must be large enough to avoid screeners recognizing images already seen. Also the managerial procedures must be followed reliably, for example ensuring that screeners actually sign out when they take a short break. The TIPS data collection system should not malfunction. Also, managers with little knowledge of statistics must beware of over-interpreting data from small samples. In fact QinetiQ in the UK has developed excellent software that helps interpret TIPS data, and specifically warns when the data are insufficient to evaluate a particular screener.

Q2. How should TSA determine the appropriate mix of technology and people in its aviation security and other modes of transportation?

A2. This is a key question in any application of Human Factors Engineering, and so is especially relevant to security systems. At the most simplistic level, my written testimony included: *"Overall, automation provides the ability to take rapid and consistent action within strict rules, while humans provide the flexibility to respond when the rules do not apply (e.g., Parasuraman, Sheridan and Wickens, 2000)."* This is a general guideline but more specific information is needed for each particular system. The Allocation of Function literature (e.g., Hollnagel, E., and Bye, A. (2000). Principles for Modeling Function Allocation. *Int. J. Human-Computer Studies.* Vol. 52, pp. 253–265) gives techniques for applying this methodology, as does the automation literature (e.g., Parasuraman, R., Sheridan, T.B. and Wickens, C.D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans,* Vol. 30 (3), May 2000). There are complete design methodologies under the headings of Socio-Technical Systems Engineering (Taylor, J.C. and Felten, D.F. (1992) *Performance by Design,* Prentice Hall) and *Cognitive Work Analysis* (Vicente, K.J. (1999). *Cognitive Work Analysis.* Mahwah, NJ: Erlbaum) which lead to specific answers in specific instances.

Note that there may be quite different appropriate mixes of technology and people in different detection systems at a single checkpoint, and certainly between different modes of transportation. The task of searching an X-ray image of a cargo container is many times more difficult for a human than searching a carry-on bag image for similar threats. Minimally-aided human search may well be an effective solution for the smaller task, but software assistance in at least the search function would probably be required for a whole container to achieve the same level of threat detection.

○