COVER BLOWN: DID TSA TIP OFF AIRPORT SCREENERS ABOUT COVERT TESTING?

FULL HEARING

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

NOVEMBER 14, 2007

Serial No. 110–86

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

49–981 WASHINGTON : 2009

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 HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

CONTENTS

COVER BLOWN: DID TSA TIP OFF AIRPORT SCREENERS ABOUT COVERT TESTING?

Wednesday, November 14, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to notice, at 10:01 a.m. In Room 311, Cannon House Office Building, Hon. Bennie G. Thompson (chairman of the committee) Presiding.

Present: Representatives Thompson, Dicks, DeFazio, Lowey, Jackson Lee, Christensen, Etheridge, Cuellar, Clarke, Green, Perlmutter, Pascrell, King, Lungren, Dent, and Bilirakis.

Chairman THOMPSON. The committee on Homeland Security will come to order. The committee is meeting today to receive testimony on TSA Tip Off is of Airport Screeners.

I want to thank our witnesses for joining us today. We are here to look into allegations that TSA tipped off airport screeners about covert testing. The Air Transport Association estimates that 27 million people will fly worldwide over the next 12 days. Since September 11th, the government has asked a lot of the public in the name of security.

Even as I speak, air travelers across the Nation are waiting in long security lines, taking off their shoes, hats and coats, putting their miniature toothpaste and shampoo in a plastic bag, even throwing perfectly good water bottles into the trash. The public has accepted these inconveniences because our government says it will lead to safer skies. So when we have TSA management tipping off airport security officials about covert testing, we have a credibility and accountability problem.

When I assumed the chairmanship of this committee, I pledged to hold the Department of Homeland Security accountable for developing a roadmap to genuine security, one that provides Americans freedom from fear. Our government cannot play on the fears of an attack and then try to cheat its way through its midterm exams.

The public has accepted increased scrutiny at our airports. In turn, the public also demands the same scrutiny of the Department and, in this case, of TSA. This is why we are holding this hearing today, to ask TSA to explain why on April 28, 2006 it used a systemwide communication system, NETHUB, to give more than 650 aviation security officials a heads-up about a possible security test.

This e-mail was provided to the committee by a member of the media and verified by my staff, that email said that several airport authorities and airport police departments have recently received

informal notice of security testing at airports around the Nation. The e-mail detailed several methods that were being used to attempt to breach airport security and even gave a brief description of some of the testers. The e-mail concluded, "We are getting the word out." But the word was not supposed to get out. Covert testing of airport security is supposed to be just that, covert.

It is hard to overstate the importance of this type of testing. It is a critical part of a layered defense that protects our Nation's commercial aviation system. Covert testers are out there trying to expose gaps before a terrorist does, and if someone at TSA undermines this testing, they are undermining aviation security as a whole.

This committee is tasked by Congress to conduct oversight of the Department of Homeland Security, its organization, and particularly transportation security programs. Today's hearing is just the first step in my committee's investigation into this issue.

To date, TSA has been very cooperative with my staff and I trust that this cooperation will continue. I hope that at the end of the road we can say that this was an isolated incident. But we will follow this investigation wherever it takes us. The flying public deserves no less.

[The prepared statement of Mr. Thompson follows:]

PREPARED STATEMENT OF THE HONORABLE BENNIE G. THOMPSON, CHAIRMAN, COMMITTEE ON HOMELAND SECURITY

The Air Transport Association estimates that 27 million people will fly worldwide over the next twelve days. Since September 11th, the government has asked a lot of the public in the name of security.

Even as I speak, air travelers across the nation are waiting in long security lines; taking off their shoes, hats and coats; putting their miniature toothpaste and shampoo in plastic bags; even throwing perfectly good water bottles into the trash. The public has accepted these inconveniences because our government says it will lead to safer skies.

So when we have TSA management tipping off airport security officials about covert testing, we have a credibility and accountability problem. When I assumed the Chairmanship of this Committee. I pledged to hold the Department of Homeland Security accountable for developing a roadmap to genuine security—one that provides Americans freedom from fear. Our government cannot play on our fears of an attack and then try to "cheat" its ways through its mid-term exams.

The public has accepted increased scrutiny at our airports. In turn, the public also demands the same scrutiny of the Department—and in this case of TSA.

That is why we are holding this hearing today—to ask TSA to explain why, on April 28, 2006, it used a system-wide communication system, NETHUB, to give more than 650 aviation security officials a head's up about a "POSSIBLE SECURITY TEST."

The email, which was provided to this Committee by a member of the media and verified by my staff, said that "several airport authorities and airport police departments have recently received informal notice" of security testing "at airports around the nation." The email detailed several methods that were being used to attempt to breach airport security, and even gave a brief description of some of the testers. The email concluded: "We are getting the word out." But the "word" was not supposed to "get out." covert testing of airport security is supposed to be just that—covert.

It is hard to overstate the importance of this type of testing; it is a crucial part of the layered defense that protects our nation's commercial aviation system.

Covert testers are out there tying to expose gaps before a terrorist does, and if someone at TSA undermines this testing, they are undermining aviation security as a whole. This Committee is tasked by Congress to conduct oversight of the Department of Homeland Security, its organization, and particularly transportation security programs. Today's hearing is just the first step in my Committee's investigation into this issue.

To day, TSA has been cooperative with my staff, and I trust that this cooperation will continue. I hope that at the end of the road we can say that this was an isolated incident, but we will follow this investigation wherever it takes us.

The flying public deserves no less.

Chairman THOMPSON. I yield 5 minutes to the Ranking Member for this committee hearing, the gentleman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

As you stated, covert testing of TSA screeners is an extremely important issue. It is a valuable tool, we all believe, to measure TSA's screening performance and identify screening vulnerabilities. As the years pass since 9/11 we will become more and more dependent on covert testing operations to challenge our TSA screening system and to improve screener training procedures and technology.

Covert testing is an effective tool when properly employed without prior notice. It is used extensively by TSA's Office of Inspection. As I understand it, all airports are subject to no-notice testing by the Office of Inspection, and that they have tested over 830 airports and conducted over 22,000 covert tests. The DHS IG also conducts hundreds of covert tests at airports independently of TSA.

In April, TSA established the aviation screening assessment program to expand covert testing internally in order to gather data to support operational decisions. In just 6 months the program has performed thousands of covert tests at hundreds of airports, testing all aspects of the screening process, including the detection of prohibited liquids and IEDs. I think all of us on the committee applaud that and the direction that TSA has taken.

These programs and the thousands of covert tests they employ seem to demonstrate that TSA believes in the value and effectiveness of this procedure to improve the U.S. Aviation screening process and ultimately our Nation's security. I think we all share this belief.

Therefore as the Ranking Member of the Subcommittee on Transportation Security Infrastructure Protection, with jurisdiction over TSA, I am extremely concerned by the implications of this morning's hearings. And so, Mr. Chairman, I look forward to the testimony of our witnesses to learn how and why TSA, if it has, has blown its cover on this covert testing program.

I was concerned when I saw the specific e-mail that the Chairman has addressed, and I am eager to hear what the response is. I might just say that in all my dealings with Mr. Hawley, I found him to be forthright with this committee and I have applauded the efforts he has made toward increasing the use of screening as a measuring tool and as an educational tool to improve the performance of our screeners, be they Federal employees or contract employees.

I also in the dealings I have had with Mr. Restovich, whose name is on this e-mail, found him to be an individual of integrity and I hold him in high regard. That is why I was mystified by this e-mail, at least the language contained in it. Hopefully we can find out exactly what occurred and what processes have been put in place to make sure it doesn't happen again, and also what actions

were taken immediately upon anybody of supervisory responsibility learning of this e-mail.

And just in ending, Mr. Chairman, I would like to say that we ought to be doing covert testing. We ought to urge and support the administration at TSA in their covert testing. It can do nothing but improve the performance of those who we had given this responsibility. And I hope what we will find is that the testing is tough testing, and increasingly tough testing, and is agile enough to respond to new threats as we see them, rather than static performance that would otherwise not be beneficial.

And so Mr. Chairman, I thank you for having the hearings and look forward to the testimony that we will receive.

Chairman THOMPSON. Thank you very much Mr. Lungren. I agree with you, we have to have covert testing. I think it is the no-notice issue that we have before us today.

[The information referred to follows:]

---Original Message---
From: NETHUB
Sent: Friday, April, 28,2006 2:51 PM
To: TSA FSD; TSA DFSD; TSA AFSDS; TSA AFSD–R; TSA AFSD–LE
Cc: TSNM COMMERCIAL AIRLINES; TSNM COMMERCIAL AIRPORTS; Schear, James; Morris, Earl R; McGowan, Morris; Restovich, Mike; Tashiro, Susan; NETHUB
Subject: NOTICE OF POSSIBLE SECURITY TEST

Date: April 28, 2006

To: Federal Security Directors

From: Mike Restovich, Assistant Administrator, Office of Security Operations

Primary POC: NetHub

Secondary POC: None

Action Due Date: None

Subject: NOTICE OF POSSIBLE SECURITY TEST

This information is provided for your situational awareness. Several airport authorities and airport police departments have recently received informal notice of possible DOT/FAA security testing at airports around the nation. Here is the text of one such notification:

> Several airports have reported that the DOT is testing airports throughout the country. Two individuals have been identified as FAA or DOT at the airport in JAX this morning. They have a stack of fake ID's, they try to penetrate security, place IED's on aircraft and test gate staff.

These individuals were in CHS earlier this week and using a date altered boarding pass managed to get through the security checkpoint. Alert your security line vendors to be aware of subtle alterations to date info. they should also pay very close attention to the photo id's being presented. They will print a boarding pass from a flight, change the date, get through security (if not noticed) and try to board a flight and place a bag in the overhead.
There is a couple, and the woman has an ID with an oriental woman's picture, even though she is Caucasian. We are getting the word out.

Office of Security Operations, NetHub

Chairman THOMPSON. Other members of the committee are reminded that under the committee rules opening statements may be submitted for the record.

I would like to welcome our distinguished panel of witnesses. Our first witness is Assistant Secretary Kip Hawley, who serves as the Administrator, Transportation Security Administration at the Department of Homeland Security. Assistant Secretary Hawley has over 20 years of experience in the private and public sectors work-

ing on various transportation and technology-related initiatives and has served since 2005.

Our second witness is Mr. Greg Kutz, managing director of the Government Accountability's Forensic Audits and Special Investigations Unit. As a senior executive at GAO Mr. Kutz has been responsible for numerous reports and testimonies relating to credit card fraud; Hurricanes Katrina and Rita; fraud, waste and abuse; transit benefit fraud; and security issues such as airport security and smuggling of nuclear materials across our Nation's border.

Our third witness is Mr. Clark Ervin, Director of Homeland Security issues at The Aspen Institute. Prior to taking his current position, Mr. Ervin served as the first inspector general of the Department of Homeland Security. During his distinguished career, Mr. Ervin has served in numerous capacities, including a stint as the Associate Director of Policy in the White House Office of National Service, under President George H.W. Bush.

Without objection, the witnesses' full statements will be inserted in the record.

Chairman THOMPSON. I now ask each of the witnesses to summarize his statement for 5 minutes beginning with Assistant Secretary Hawley.

STATEMENT OF THE HONORABLE EDMOND S. "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Mr. HAWLEY. Thank you, Mr. Chairman, Mr. Lungren, members of the committee. I appreciate the opening statements that you both made. And Mr. Chairman, the only thing I would change in yours is where it said "when" TSA does tipping off to "if." And I think if TSA were to be doing tipping off of covert testing, that would indeed be a serious matter.

I would like to make very clear that the matter is under investigation now, but there is nothing that I have learned in the past week and a half or since I was first made aware of this e-mail that would indicate there was any intent on anybody's part associated with that e-mail to do covert testing or tip-off. So there is no tip-off and no cheating.

This is very important to us because covert testing is part of our fiber as an Agency. As you both mentioned, it is how we stay ahead of terrorists with efforts to do IEDs at the checkpoint. And we do over 70,000 electronic tests a day on our work force. And we do 2,500 actual bomb component covert testing at checkpoints. That means every checkpoint, every shift, every day, every one of the 450-some airports that we have. They have actual bomb components, they put them through the checkpoint. That is a massive amount of testing. This is the most tested work force that I know of in the United States and it uses the best technology, and I have to say that they are the best in the world at what they do. So any allegation about integrity associated with that process would indeed be extremely serious.

I would just like to make mention of Mr. Restovich. The 9/11 Commission has very much of value in their report. And one of the things that I want to highlight is to talk about information sharing, particularly with people at the edge of a network such as our Fed-

eral Security Directors around the system. When Mike took over as head of security operations in January or February 2006, one of his initiatives was to create something called NETHUB that would be able to quickly send out information to the edge of our network, the Federal Security Directors. That is the organization that sent out the e-mail.

The individual who sent out the e-mail in question had no knowledge of covert testing that the IG was at that point performing at TSA. The individual who sent that e-mail had no knowledge of covert testing. Mike Restovich, when he found out about it—he was not the author of the e-mail—when he found out about it, immediately had it recalled. The elapsed time from when it was sent to when it was recalled was 13 minutes. There was no intent to tip off. There was no cheating. And when the facts are completely in and the investigation is over, I think we are going to find out that there is not a cheating problem or a tip-off problem.

This is so important to us, because integrity is the center of everything we do with the American public. And just the allegations themselves got worldwide coverage as if there were cheating at TSA. That was read by our partners abroad, it was read by our enemies abroad, and it was read by our employees. And that is damage that is lasting, because when this whole issue is over, I think there are many interesting issues that are worth pursuing, but it is not a question of cheating. And a rush to judgment on that I think does a disservice not only to our people, to the members of the TSA work force, but also to our flying public.

So I look forward to discussing, as I have in the past and will continue to do openly, take the criticism. But I think you know as members of this committee, that when we do have issues, we get on them and we fix them. And if there are issues related to this that come up during the course of that investigation, we will get on them and we will fix them. But I want to make very clear right now, there is not an integrity issue that is risen from anything I know from this e-mail at this point. Thank you, sir.

Chairman THOMPSON. Thank you very much.

[The prepared statement of Mr. Hawley follows:]

PREPARED STATEMENT OF THE HONORABLE EDMOND S. "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Good morning Chairman Thompson, Ranking Member King, and distinguished members of the Committee. Thank you for this opportunity to discuss the covert testing of security screening checkpoints at airports.

Overview of Covert Testing

Since it assumed responsibility for aviation security screening at airports, the Transportation Security Administration (TSA) has always recognized the value and importance of covert testing to measure TSA's screening performance and identify areas that require improvement. Covert testing is a tool to identify vulnerabilities in the system and uncover weaknesses of training, procedures or technology. The primary purpose of covert testing is not to test an individual officer or airport, but to act as a measure of system-wide effectiveness and drive improvement through training, procedures, and technology.

Covert testing of TSA's screening operations is performed by several organizations within the Department of Homeland Security (DHS): TSA's Office of Inspection (OI), the Office of Inspector General Office, and TSA's Office of Security Operations (OSO).

OI conducts extensive covert tests around the nation with no notice to local or headquarters officials. These expert testers are trained in the latest methods of

smuggling bombs, bomb parts and weapons through checkpoints using techniques acquired by national and international intelligence partners and gathered through years of experience. The OI covert testing staff includes former Transportation Security Officers (TSO) who have on-the-ground experience in screening passengers. Airports are selected based on a number of factors, including intelligence reports, threats to aviation, and the airport environment. All airports are subject to no-notice testing by OI. To date, OI has tested at over 830 airports and conducted in excess of 22,000 covert tests. In 2008, OI will conduct over one thousand covert tests, continually restructured to reflect the current terrorist threat, at over 100 airports to assess our security vulnerabilities. For safety purposes airport law enforcement are notified prior to testing. Once testing starts, TSA management is made aware of the situation in accordance with established policies and protocols, which do not permit advanced notice to TSOs and who are thus subjected to no-notice testing. After testing is completed, agents discuss the results with TSOs and local TSA officials and provide additional training to TSOs to raise vulnerability awareness and improve security operations.

In addition to OI testing, DHS IG also conducts hundreds of covert tests at airports from coast to coast and acts completely independently from TSA. DHS IG agents measure the effectiveness of screening protocols and communicate these results to TSA and the Department in order to increase effectiveness of screening and security. TSA uses these independent results to validate and improve training.

Beginning in April of this year, TSA established the Aviation Screening Assessment Program (ASAP) within OSO to greatly expand our internal covert testing and provide statistically sound data to support operational decisions. This program arose out of a recognition that, notwithstanding the valuable information learned from the extensive covert testing conducted by OI and others, TSA nevertheless needed a more systematic framework to more accurately assess the effectiveness of our screening process and to identify which aspects of the process require improvement. This program has performed thousands of covert tests at hundreds of airports nationwide in just six months. We are testing virtually every aspect of the screening process, including the detection of prohibited liquids and improvised explosive devices (IEDs).

Under separate training programs, TSA additionally conducts over a thousand covert exercises focused on detecting IEDs and almost 70,000 electronic image tests—*every day*. The information collected from these programs enables TSA to make informed decisions based on reliable data to better target our efforts to improve the screening process. ASAP will enhance our ability to identify which aspects of the screening process needs improvement: operations, procedures, technology, training, or management. And, we now have a formal process to conduct a thorough assessment of the screening process every six months and implement the appropriate courses of action to address any concerns revealed during the expansive covert testing.

Because of this array of testing efforts, our TSOs are among the most tested workforce in the country. TSOs are literally tested every day, on every shift, at every checkpoint in every lane across over 400 airports around the United States.

Maintaining the Integrity of Covert Testing

I would also like to address concerns raised by recent media reports on the integrity of the covert testing of screening operations. The value of covert testing relies upon the testers' ability to perform unannounced tests. We take great care to protect the covert nature of the testing to ensure the data is an accurate measure of the screening system's performance. We treat covert testing results very seriously because these results help us identify vulnerabilities in the system and implement corrective measures to prevent another terrorist attack. We routinely provide very limited notice to local law enforcement in certain circumstances involving real threat items for safety reasons so as to avoid endangering airline passengers, flight crews, and our own workforce which, unbeknownst to any of them, are in the immediate area of a covert test. TSOs should not be given advanced notice of covert testing. Indeed, advanced notice to TSOs from a TSA employee is a violation of established policies and protocols, and defeats the purpose of covert testing.

Mr. Chairman, I understand that you are aware of a specific matter involving a TSA-internal "NETHUB" communication on April 28, 2006, currently under investigation by the DHS IG. We are fully cooperating with the investigation and will appropriately address any findings of the investigation. NETHUB is a division within TSA's Office of Security Operations created in the spring of 2006 that serves a central communications conduit between TSA Headquarters and our field operations at over 400 airports. NETHUB sends and receives communications by email, telephone and fax on operational and administrative matters, such as distributing new

screening procedures and security directives, announcing opportunities for employees to serve on national advisory councils, and various data requests from field operations.

Conclusion

In addition to Innovation and Team Spirit, Integrity is one of the three core values of TSA. We require our personnel to conduct themselves in an honest, trustworthy and ethical manner at all times. Maintaining the integrity of covert tests of our screening operations is essential for TSA to gain the type of information necessary to continually improve and adapt our screening processes to stay ahead of terrorists. Any individual action to compromise the integrity of covert testing is extremely short-sighted and contrary to TSA's mission of providing an effective security system to protect aviation.

Chairman Thompson, thank you again for the opportunity to testify today. I am happy to respond to the Committee's questions.

Chairman THOMPSON. We now recognize Mr. Kutz for 5 minutes.

STATEMENT OF GREGORY KUTZ, MANAGING DIRECTOR, OFFICE OF FORENSIC AUDITS AND SPECIAL INVESTIGATIONS, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. KUTZ. Mr. Chairman and members of the committee, thank you for the opportunity to discuss covert testing. All covert testing at GAO is done by my unit, which is called Forensic Audits and Special Investigation, or FSI. My testimony today has two parts: first, how we do covert testing; and second, specific examples of our work.

First we follow both investigative standards and more detailed FSI procedures for our operations. Our covert testing is typically done at the request of congressional committees and subcommittees. As &1 Legislative branch agency working for the Congress, we are independent of th. Executive branch agencies that we test.

FSI conducts covert tests as a red team operation, meaning that we do not notify agencies in advance of our testing. In contrast, blue team operations involve notifying agency officials in advance. All FSI investigations have a written plan. Well-trained, experienced people are critical to the success of a covert test. The average FSI investigator that does our covert testing has over 20 years of law enforcement experience. Plans must be approved by the FSI Assistant Director for Investigations, me, and two other executive committee members at GAO before testing begins.

We require investigators acting in a covert capacity to have a cover team to ensure safety. If a covert operation is uncovered during the testing, the cover team is to identify themselves and alert law enforcement officers or others that we are conducting a test. We use only publicly available information to develop our covert tests. This approach provides the most realistic test of what a terrorist or criminal might actually do. For example, when making counterfeit documents, we use only publicly available hardware, software, and materials.

Once the operation is complete, we first brief our congressional requesters, we then brief Agency officials and provide suggestions to address any specific weaknesses that we identify. Finally, we issue a report and often times will testify before our congressional requesters.

Moving on to my second point, we have conducted a wide variety of covert testing for many different congressional committees and subcommittees across the Congress. Examples of various testing in-

clude controls over radioactive materials, border security, airport security, sales of sensitive military technology and fraud prevention controls over Federal programs.

The following three examples provide more details. First, using a bogus business and fictitious individuals, we obtained a genuine radioactive materials license from the Nuclear Regulatory Commission. We altered this license and used it to obtain commitments to ship to our bogus business dangerous amounts of radioactive materials that could be used to make a dirty bomb.

Second, posing as defense contractors, we were able to penetrate two DOD excess property warehouses. There we obtained $1.1 million of surplus military property that was sensitive military technology. Our cover story was so convincing that the DOD employees, including contractors, helped us to identify targeted items and load them into our rented van.

And third, posing as victims of Hurricane Katrina and Rita, our investigators applied for Federal assistance using false identities, bogus addresses, and fabricated disaster stories. FEMA sent our bogus victims a number of checks based upon these bogus applications. In case you are wondering, we gave the checks back to FEMA after our test.

In conclusion, our covert testing provides the Congress with irrefutable evidence about Federal agencies under live conditions. The results of our covert testing have also been used by Federal agencies across the government to strengthen homeland and national security and to minimize fraud, waste, and abuse of taxpayer dollars.

Mr. Chairman, this ends my statement, I look forward to your questions.

Chairman THOMPSON. And I am sure you will have some questions from that.

[The prepared statement of Mr. Kutz follows:]

United States Government Accountability Office

GAO

Testimony

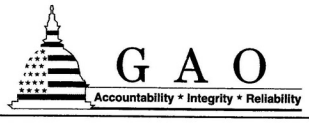
Before the Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, November 14, 2007

INVESTIGATIVE OPERATIONS

Use of Covert Testing to Identify Security Vulnerabilities and Fraud, Waste, and Abuse

Statement of Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations



GAO-08-286T

November 14, 2007

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-08-286T, a testimony before the Committee on Homeland Security, House of Representatives

INVESTIGATIVE OPERATIONS

Use of Covert Testing to Identify Security Vulnerabilities and Fraud, Waste, and Abuse

Why GAO Did This Study

GAO's Forensic Audits and Special Investigations team (FSI), which was created in 2005 as an interdisciplinary team consisting of investigators, auditors, and analysts, conducts covert tests at the request of the Congress to identify vulnerabilities and internal control weaknesses at executive branch agencies. These vulnerabilities and internal control weaknesses include those that could compromise homeland security, affect public safety, or have a financial impact on taxpayer's dollars. FSI conducts covert tests as "red team" operations, meaning that FSI does not notify agencies in advance about the testing.

Recently, concerns have arisen as to whether top management at the U.S. Transportation Security Administration (TSA) were negatively impacting the results of red team operations by leaking information to security screeners at the nation's airports in advance of covert testing operations. Consequently, GAO was asked to (1) briefly explain FSI's processes and procedures concerning covert testing and (2) provide examples of covert activities performed.

To view the full product, including the scope and methodology, click on GAO-08-286T. For more information, contact Gregory D. Kutz at 512-6722 or kutzg@gao.gov.

What GAO Found

FSI has strict internal procedures related to the planning, execution, and reporting of covert activities. First, FSI and senior GAO management decide on a case-by-case basis whether engagements requiring covert tests are within the scope of GAO's authority. Next, FSI identifies the aspects of the security system or the government program that are particularly vulnerable to terrorist threats or fraudulent activities and relies on the experience of its investigators to develop a written investigative plan. This plan typically includes the creation of fictitious identities and counterfeit documentation. All counterfeit documents that FSI uses are manufactured using hardware, software, and materials that are available to the general public—this allows FSI to demonstrate that any security vulnerabilities it finds could be exploited by a criminal or terrorist with moderate means and resources and would not require sophisticated insider knowledge.

FSI's investigators are the only GAO staff allowed to participate in the execution phase of testing, although audit and analyst staff are often involved in planning and operational support. Importantly, if investigators discover vulnerabilities that pose a significant and immediate threat to public safety, FSI immediately will discontinue its investigation and alert the appropriate government law enforcement agency. Once the operation is complete, FSI conducts a "corrective action briefing" with officials at the tested entity to report that they have been the subject of a covert operation, share the results of the testing and, if necessary, suggest potential remedies for any identified control weaknesses or security vulnerabilities.

The following summarize recent FSI red team operations. These operations provided the Congress with irrefutable evidence about the actual ability of federal agencies under "live" conditions to deal with security threats and to protect government assets from fraudsters.

- Using counterfeit documents and posing as employees of a company with a Nuclear Regulatory Commission license, FSI investigators successfully crossed the U.S. northern and southern borders with the type of radioactive materials that could be used to make a dirty bomb.
- Posing as private citizens, FSI investigators purchased sensitive military equipment—including ceramic body armor inserts, guided missile radar test sets, and microcircuits used in F-14 fighter aircraft—on the Internet from the Department of Defense's liquidation sales contractor.
- Using bogus driver's licenses, FSI investigators successfully gained entry to all 24 Department of Transportation regulated urine collection sites that FSI tested, which are responsible for providing drug testing of commercial truck drivers in safety sensitive transportation positions.
- Using false documents and an erroneous IRS taxpayer identification number, FSI pretended to be a charity and successfully applied to three of the Combined Financial Campaign's local 2006 campaigns.

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to discuss covert testing activities conducted by the Forensic Audits and Special Investigations (FSI) unit of the GAO. FSI, which was created in 2005 as an interdisciplinary team consisting of investigators, auditors, and analysts, conducts covert tests at the request of the Congress. The objectives of these tests are to identify security vulnerabilities and internal control weaknesses at executive branch agencies, including those that could compromise national or homeland security, affect public safety, or have a financial impact on taxpayer's dollars. In brief, my remarks today relate to the processes and procedures FSI uses to conduct this work and the results of some of our operations.

FSI's covert testing operations are typically part of a broader security vulnerability assessment or a forensic audit designed to identify fraud, waste, and abuse related to federal programs. FSI conducts covert tests as "red team" operations, meaning that for these operations, FSI does not notify agencies in advance about our testing. As an example, in 2002 we conducted a red team operation to evaluate the security of federal buildings in Atlanta, Georgia.[1] In this case, we obtained genuine security badges through deception and then counterfeited the badges, allowing several investigators to access the buildings without the knowledge of security personnel or agency officials. In contrast, "blue team" operations involve notifying affected agencies in advance about testing; GAO information technology specialists test executive branch agencies' computer systems using a blue team approach. Although both types of operations uncover valuable information, we are confident that the red team approach provides the Congress with dependable, irrefutable evidence about the actual ability of federal agencies under "live" conditions to deal with security threats and to protect government assets and programs from fraudsters.

Recently, concerns have arisen as to whether top management at the U.S. Transportation Security Administration (TSA) were negatively impacting the results of red team operations by notifying security screeners at the nation's airports in advance of covert testing operations. Consequently, you requested that we (1) briefly explain FSI's processes and procedures

[1]GAO, *Security Breaches at Federal Buildings in Atlanta, Georgia*, GAO-02-668T (Washington, D.C.: Apr. 30, 2002).

concerning covert testing and (2) provide examples of covert activities we performed and the results.

FSI Covert Testing Processes and Procedures

Because of the sensitive nature of our work, and the fact that our findings can generate information that may compromise national or homeland security, we apply strict processes and procedures when performing covert work. FSI plans and conducts all investigations in accordance with the standards established by the President's Council on Integrity and Efficiency (PCIE). These standards are relevant to the full range of government investigations, including fraud, corruption, white-collar crime, security inquiries, whistleblower issues, and other special investigations. With regard to covert operations specifically, FSI has developed our own internal procedures detailing the requirements related to the planning, execution, and reporting phases of the operations.

Planning a Covert Test

FSI, in conjunction with senior-level GAO management, decides on a case-by-case basis whether to accept written congressional requests requiring covert operations or whether to incorporate covert testing into existing engagements. In making these decisions, a number of factors are considered, including, but not limited to, whether the proposed operations are within the scope of GAO's authority; whether the operations may be performed more appropriately by agency Inspectors General; and whether the requested work presents significant risk of personal injury to individuals or other harm to persons, businesses, or public safety. We also identify the specific aspects of the security system or the government program that are particularly vulnerable to terrorist threats or fraudulent activities. Once the use of covert operations is accepted, the first step in FSI's process involves using the training and experience of our investigators to develop a written investigative plan. Because the average FSI investigator has over 20 years of law enforcement experience, they are uniquely positioned to develop a blueprint for performing the work, while minimizing disruption to the day-to-day operations of the agency being tested and seeking to ensure the safety of all involved.

In general, FSI investigative plans contain the following elements: a statement regarding the investigation's overall objectives; a description of the legal issues involved; and a summary of the allegations that merit investigation or the processes, systems, and controls that will be tested. When covert operations are involved, the plan must also contain a detailed outline of the steps that would be necessary to effectively conduct the operation. In most cases, this step-by-step process will include the

creation of fictitious identities and counterfeit documentation, including items such as birth certificates, driver's licenses, credit cards, billing records, and social security cards. All counterfeit documents that FSI uses are manufactured by FSI using hardware, software, and materials that are available to the general public—this allows us to demonstrate that any security vulnerabilities we find could be exploited by a criminal or terrorist with moderate means and resources and would not require sophisticated insider knowledge or access to sophisticated equipment. In order to obtain the best possible evidence, the plan may also request that GAO management authorize FSI to obtain photographs or video or audio recordings. The investigative plan must be reviewed and approved by an FSI Assistant Director for Investigations, FSI's Managing Director, and two members from GAO's top management team.

Executing a Covert Test

Once the investigative plan has been approved, FSI proceeds with the covert operation. In general, FSI's investigators are the only staff allowed to participate in actual testing activities, although audit and analyst staff are often involved in planning and operational support. Furthermore, if the covert testing is conducted outside GAO headquarters (e.g., the testing of U.S. border security), FSI policy requires that investigators acting in a covert capacity have a "cover team" of investigators to ensure safety. These agents are usually placed strategically about the test site to monitor the situation and to alert the investigators conducting the tests if anything seems out of place. The responsible Assistant Director for Investigations is also present during all covert operations conducted outside of the GAO headquarters building. Before any testing begins, the Managing Director generally receives an itinerary sheet with all the names of the investigators involved and pertinent contact numbers.

During the execution phase, investigators are required to protect investigative information from unauthorized disclosure, protect the rights of all individuals involved, and avoid any action that may give the appearance of coercion or intimidation. In addition, investigators must safeguard any counterfeit documentation against theft or damage. Investigators must document all evidence obtained in accordance with PCIE standards and applicable FSI and GAO policies.

Investigators routinely make dry runs of covert operations tests to determine whether new or enhanced security procedures have been implemented after the development of our testing plan. Because FSI only uses publicly available information to develop our covert tests and does not consult with agency insiders, the specifics of our operations are not

leaked to agency officials. Our belief is that by using only publicly available information, our tests reveal what an actual terrorist or criminal might do during a real security breach or fraud scheme.

Furthermore, our policy is that if an FSI covert operation is uncovered during one of our tests, the backup investigators immediately will identify themselves and alert the proper law enforcement authorities that a test is being conducted and identify all participants as being FSI investigators with the proper authority. Importantly, if investigators discover vulnerabilities that pose a significant and immediate threat to public safety, FSI immediately discontinues its investigation and alert the appropriate government law enforcement agency. Under no circumstances will FSI make publicly available any photograph, videotape, or audiotape that could be used as a road map by criminals or terrorist groups.

Reporting the Results of Covert Testing

Once the operation is complete, investigators immediately brief the congressional requester. Next, FSI conducts a "corrective action briefing" with officials at the tested entity to inform them that they have been the subject of a covert operation, share the results of the testing , and, if necessary, suggest potential remedies for any identified control weaknesses or security vulnerabilities.

After all parties have been briefed, FSI will issue a report or testimony that comports with PCIE and applicable FSI and GAO standards. Because the covert testing is sometimes part of a broader forensic audit, parts of the product may also adhere to U.S. generally accepted government auditing standards. These products contain our findings, the results of the corrective action briefing with the tested entity, and sometimes contain recommendations to agency management. FSI does not usually reveal all details about its covert methodologies in public products. For example, we typically do not reveal the name of any bogus companies that we create or the fictitious identities that we use. Moreover, if our findings relate to issues of national or homeland security, FSI submits a draft product to the agency for a sensitivity review prior to issuance. In some cases, FSI products are issued in conjunction with letters to the tested entity or other law enforcement agencies referring specific instances of wrongdoing, including the criminal activities of agency officials or private citizens.

Examples of FSI Covert Testing

At the request of a number of different congressional committees and subcommittees, FSI has conducted a wide variety of covert testing activities, including evaluations of controls over radioactive materials and security at America's borders, airport security, sales of sensitive and surplus military equipment, public safety, and other issues including fraud prevention controls over federal programs. As demonstrated by the examples below, covert activities are instrumental in identifying important weaknesses that expose the federal government—and most importantly, the American public—to threats to their security and safety, as well as fraud, waste, and abuse related to taxpayer dollars. Following are summaries of several covert activities we performed in recent engagements and the results we obtained.

Controls over Radioactive Materials and Security at America's Borders

The covert activities we performed in these areas include:

- Using the name of a bogus business that existed only on paper, FSI investigators obtained a genuine radioactive materials license from the Nuclear Regulatory Commission (NRC) without leaving the office or actually meeting with or having our nonexistent facility inspected by anybody from the NRC.[2] After altering the maximum quantity of materials listed on the license, FSI investigators faxed these licenses to two suppliers and obtained price quotes and commitments to ship machines containing radioactive materials in quantities that could have been used to produce a dirty bomb. In contrast, a state allowed by the NRC to issue radioactive licenses indicated that it would perform physical verification prior to approving a radioactive materials license for our bogus company. As a result, we informed NRC that we had "financial problems" and withdrew our application.

- Using counterfeit documents and posing as employees of a company with an NRC license, FSI investigators successfully crossed the northern and southern borders with the type of radioactive materials that could be used to make a dirty bomb.[3] While the radiation portal monitors at the two border locations properly signaled the presence of the radioactive materials in our vehicles, the inspectors readily

[2]GAO, *Nuclear Security: Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Sources Are Not Effective*, GAO-07-1038T (Washington D.C.: July 12, 2007).

[3]GAO, *Border Security: Inspectors Transported Radioactive Sources across Our Nation's Borders at Two Locations*, GAO-06-583T (Washington, D.C.: Mar. 28, 2006).

accepted our counterfeit documents—including a counterfeit bill of lading and NRC license—which we created using publicly available hardware, software, and materials. As part of this operation, an FSI investigator using the name of a fictitious company ordered by telephone a small amount of radioactive sources to "calibrate personal radiation detection pagers." These radioactive sources were shipped to the Washington, D.C., area to the fictitious company. This test demonstrated that anyone could purchase small quantities of radioactive sources for stockpiling.

- Posing as individuals with simulated contraband including radioactive material, FSI investigators successfully crossed the northern U.S. border at locations that were unmanned and unmonitored.[4] This test showed that the northern border is significantly vulnerable to terrorists or criminals entering the United States undetected.

Airport Security Testing

- In 2006, we reported on the results of covert security vulnerability testing of numerous airports across the country. During these covert tests, our investigators passed through airport security checkpoints carrying prohibited explosive components without being caught by Transportation Security Administration (TSA) security officers. The details of this March 2006 report are classified; however, TSA has authorized this limited discussion.

Sale of Sensitive and Surplus Military Equipment

- Posing as private citizens, FSI investigators purchased sensitive military equipment—including ceramic body armor inserts, guided missile radar test sets, and microcircuits used in F-14 fighter aircraft—on the Internet from the Department of Defense's (DOD) liquidation sales contractor.[5] Some of these items required us to obtain an "end use certificate", which is intended to provide assurance that sensitive property is sold to legitimate buyers. To obtain these parts we applied for this certificate using fictitious individuals and bogus documents. Subsequently, a DOD official called our investigator (the fictitious individual) asking why he had no credit or other history. Our investigator used social engineering and a copy of a bogus utility bill to

[4]GAO, *Border Security: Security Vulnerabilities at Unmanned and Unmonitored U.S. Border Locations*, GAO-07-884T (Washington, D.C.: Sept. 27, 2007).

[5]GAO, *DOD Excess Property: Control Breakdowns Present Significant Security Risks and Continuing Waste and Inefficiency*, GAO-06-981T (Washington, D.C.: July 25, 2006).

address the questions and our application was then approved. We used this certificate to buy items, including F-14 parts, which are in demand by Iran, the only country currently operating F-14 fleet in the world.

- FSI investigators posing as DOD contractor employees were able to easily penetrate two Department of Defense excess property warehouses. There, they were able to obtain about $1.1 million in sensitive military equipment items, including launcher mounts for shoulder-fired guided missiles, body armor, a digital signal converter used in naval surveillance, and an all-band antenna used to track aircraft. Our cover story was so convincing that DOD and its contractor staff helped our investigators locate targeted items and load them into our rented van.

Public Safety

- Using bogus driver's licenses, FSI investigators successfully gained entry to all 24 Department of Transportation regulated urine collection sites that we tested, which are responsible for providing drug testing of commercial truck drivers in safety sensitive transportation positions.[6] This test shows that individuals required to undergo drug testing can send someone to take a drug test in their place using fake identification. Furthermore, FSI investigators were able to use adulterants at four collection sites and substitute synthetic urine at another four sites without being caught by site collectors. None of the eight synthetic or adulterated urine specimens were detected by the labs.

Other Testing

Activities in this area include obtaining disaster assistance and demonstrating weaknesses in agencies' fraud prevention controls.

- Posing as disaster victims of hurricanes Katrina and Rita, FSI investigators applied for federal assistance using falsified identities, bogus addresses, and fabricated disaster stories to register for assistance under the Individuals and Households Program.[7] Despite the fact that our applications over the Internet were not accepted because

[6]GAO, *Drug Testing: Undercover Tests Reveal Significant Vulnerabilities in DOT's Drug Testing Program*, GAO-08-225T (Washington, D.C.: Nov. 1, 2007).

[7]GAO, *Expedited Assistance for Victims of Hurricanes Katrina and Rita: FEMA's Control Weaknesses Exposed the Government to Significant Fraud and Abuse*, GAO-06-403T (Washington, D.C.: Feb. 13, 2006).

of data validation procedures the Federal Emergency Management Agency (FEMA) had implemented, FSI investigators successfully registered over the phone. As a result, FEMA sent a number of checks to FSI for our fictitious individuals based on our bogus applications. After our investigation was complete, we returned the checks we obtained.

- Using easily obtained data on the Internet, FSI submitted a fictitious travel order for a fictitious individual to a DOD commercial travel office to obtain an airline ticket from Washington, D.C., to Atlanta, Georgia.[8] DOD issued FSI the airline ticket, established an obligation, and paid for the ticket without detecting the fictitious nature of the request. On the day of the scheduled flight, an FSI investigator went to the airline's ticket counter at the airport and, under the name of this fictitious individual, picked up a boarding pass.

- Using entirely false documents and an erroneous IRS taxpayer identification number, FSI pretended to be a charity and applied to three of the Combined Financial Campaign's local 2006 campaigns.[9] The fictitious entity was accepted into all three CFC campaigns. Immediately after our applications were accepted, we notified CFC officials and withdrew our charity from the campaigns in order to prevent federal employees from making donations to our fictitious charity.

Conclusions

The results of FSI's covert testing have been used by Congress and federal agency managers across the government to help strengthen homeland security and minimize fraud, waste, and abuse of taxpayer dollars. We will continue to offer this valuable service to the Congress in a responsible and professional manner and provide the results of our work to agency management, where appropriate, so that they can take concrete steps to improve the federal government's operations.

[8]GAO, *DOD Travel Cards: Control Weaknesses Led to Millions in Fraud, Waste, and Improper Payments*, GAO-04-825T (Washington, D.C.: June 9, 2004).

[9]GAO, *Tax Debt: Some Combined Federal Campaign Charities Owe Payroll and Other Federal Taxes*, GAO-06-755T (Washington, D.C.: May 25, 2006).

Mr. Chairman and Members of the Committee, this concludes my statement. I would be pleased to answer any questions that you or other Members of the Committee may have at this time.

Chairman ERVIN. Mr. Ervin for 5 minutes.

STATEMENT OF CLARK KENT ERVIN, DIRECTOR, HOMELAND SECURITY PROGRAM, THE ASPEN INSTITUTE

Mr. ERVIN. Thank you very much, Mr. Chairman and members. For this invitation to testify at this very important hearing today. I have a longer statement that I have submitted for the record. I will summarize that statement for you now.

The April 2006 e-mail from TSA to Federal Security Directors and other security personnel around the country alerting screeners to covert testing, as troubling as it is on its face, appears to be part of a pattern at both Federalized airports and privately run ones.

About 2 years ago, as you will recall, a former employee for the San Francisco contractor, Covenant, alleged that undercover tests were compromised in this fashion there. Those claims were substantiated by DHS Office of Inspector General investigation last fall. At a Federalized airport, the one in Jackson, Mississippi, DHS OIG has substantiated allegations that TSA employees and even TSA management compromised undercover tests by alerting screeners beforehand there.

During my time as inspector general at the Department of Homeland Security during the covert test that we conducted at both Federalized and privatized airports all around the country in 2002 and 2004, on occasion our testers got the impression that their tests were compromised. We were never able to substantiate that, but against this pattern it appears in fact to have been the case. I should mention that I have been told by those who have seen the results of the testing that is the subject of today's hearing that the results were dismal. If screeners still failed tests they knew were being conducted, heaven help us when al-Qa'ida next probes for weaknesses in aviation security.

It is urgent that Congress and the independent DHS Office of Inspector General investigate this matter thoroughly. If the facts are as they appear to be on their face—and it would seem to me to be a very heavy burden to prove otherwise—then the person who sent this e-mail, any person or people who authorized it and those who knew about it in advance, did nothing to stop it from being sent, and anyone who received it and acted on it should all be summarily fired and then criminally prosecuted for potentially endangering the security of the United States.

I understand that poor test results are embarrassing to TSA and its senior managers. And I understand that human nature being what it is, people don't like to be embarrassed. But the security of the Nation must come before protecting reputations. If these tests are compromised and people are led to believe that screeners are better at detecting concealed weapons than they are, terrorists can exploit this gaping hole in our security to kill thousands more people someday.

There should be no mystery as to what it takes to improve screener performance significantly. The recommendations that my former office made 4 years ago remain as valid today as they were then. Screeners need to be trained regularly and stringently under conditions that approximate real-world ones as closely as possible. Screeners whose performance is consistently subpar must ulti-

mately be fired. Supervisors must be evaluated on the basis of their success or failure in training their teams. Supervisors whose teams consistently perform in a subpar fashion must ultimately be fired. And technologies like Backscatter that can see through clothing and spot concealed guns and knives, and multiview X-ray technology that automatically rotates bags in a three-dimensional fashion, ultimately revealing concealed weapons, must finally be moved beyond the testing and pilot phase to widespread deployment.

It may be impossible to spot concealed weapons 100 percent of the time, but through better training, closer supervision and more widely deployed sophisticated technology, we can come as close to 100 percent detection as humanly possible. All these many years after 9/11 we still have failed to grasp that airport screeners are our very last line of defense before another group of hijackers attempt to board planes and carry out another devastating attack on our homeland.

TSA is compromised if screener testing endangers the security of the Nation. As I said, everyone responsible for this particular compromise and any others that may have occurred over the years should be subjected to the maximum penalty allowed by law. Thank you very much.

Chairman THOMPSON. Thank you very much for your testimony.

[The prepared statement of Mr. Ervin follows:]

PREPARED STATEMENT OF CLARK KENT ERVIN

Thank you Mr. Chairman, Mr. King, and members for inviting me to testify today at this important hearing. Given my background as the Department of Homeland Security's first Inspector General and my present work as the Director of the Homeland Security Program at the Aspen Institute, I am often asked whether in my judgment America is safer today than we were on 9/11. The answer to that question is yes, especially in the area of aviation. Given the enormity of that tragedy and our tendency "to fight the last war" rather than to anticipate the next one, the bulk of our attention and resources have been focused on that sector. The good news is that we have something to show for it—cockpit doors are hardened; some pilots are armed; and the number of air marshals is significantly higher.

The bad news is that in several significant respects we remain far more vulnerable to another catastrophic terror attack from the air than we should be all these many years after 9/11, the creation of TSA, and the creation of the Department of Homeland Security. None of these respects is more critical than that of airport screener performance in terms of their ability to spot concealed guns, knives, and explosives.

The sad fact is that for all the dollars and attention that has been focused on screener performance since 9/11 study after study—by the DHS Inspector General, the Government Accountability Office; news organizations, and, even, the TSA itself—shows that it is just as easy today to sneak these deadly weapons past screeners than it was on 9/11.

The first major briefing I had as Inspector General of DHS when I arrived in 2003 was with my counterpart at the Department of Transportation, Ken Mead, in whose jurisdiction aviation security lay prior to the creation of DHS. At the request of the President himself immediately after the 9/11 attacks, Mead sent teams of undercover auditors to airports around the country—large and small—to test the ability of the then privatized screener workforce to spot concealed weapons. Those results are still classified nearly seven years later, but suffice it to say that it was far easier than it should have been to sneak these weapons through in the immediate aftermath of 9/11 when screeners' alert level should have been at its highest. The first major project I then asked my own audit team to undertake in 2003 was to go to the very same airports as Mead's teams had done two years earlier to see whether the federalization of the screener workforce; the creation of TSA; and the transfer of TSA from the DOT to DHS had made any difference in screeners' ability to spot deadly weapons. When the results came in in late 2003/early 2004, they were exactly the same, to the decimal point, as those Mead's teams obtained in 2001. Before

departing DHS in 2004, I sent my teams out again to the same airports to see whether the recommendations we had made in terms of training, supervision, and technology (about which more later) had made any difference. The results came in in the spring of 2005, and they, too, were exactly the same as those obtained four years earlier. The pattern has continued all across the country to the present day. There is the GAO report last spring to the effect that investigators were able to sneak potential bomb components through checkpoints at 21 different airports. There was a news report last fall that screeners at Newark International Airport, not incidentally one of the airports transited by the 9/11 hijackers, failed 20 out of 22 undercover tests. And, then, of course, there was the USA story a couple of weeks ago reporting that screeners failed TSA's own undercover tests 75% of the time at LAX, and 60% of the time at Chicago O'Hare.

Interestingly that same study found only a 20% failure rate at San Francisco airport. San Francisco happens to be one of the handful of airports around the country where screeners continue to be private contract employees. One might think that such a dramatically better result at a privately run airport suggests that such airports are better at training screeners than federalized ones. I caution against that conclusion, at least not a priori. Our work during my time at DHS showed no appreciable difference in screener performance between federalized airports and privatized ones.

Another possible explanation for the discrepancy relates to the subject of today's hearing—the possibility that TSA may have tipped off screeners to the presence of undercover investigators. About two years ago, a former employee for the San Francisco contractor, Covenant, alleged that undercover tests were compromised in this fashion. Those claims were substantiated by a DHS Office of Inspector General investigation last fall.

At a federalized airport, the one in Jackson, Mississippi, DHS OIG has substantiated allegations that TSA employees, and even TSA management, compromised undercover tests by alerting screeners beforehand.

So, the April 28, 2006, email from TSA to Federal Security Directors and other security personnel around the country alerting screeners to covert testing may well be part of a pattern at both federalized airports and privately-run ones. (I should mention that I have been told by those who have seen the results of this testing that the results were dismal. If screeners still fail tests that they know are being conducted, Heaven help us when al-Qa'ida next probes for weaknesses.)

It is urgent that Congress and the independent DHS Office of Inspector General investigate this matter thoroughly. The person who sent this email, any people who authorized it and those who knew about it in advance and did nothing to stop it from being sent; and anyone who received it and acted on it should all be summarily fired and criminally prosecuted for potentially endangering the security of the United States. I understand that poor test results are embarrassing to TSA and its senior managers, and I understand that people don't like to be embarrassed. But, the security of the nation must come before protecting one's reputation. If these tests are compromised, and people are led to believe that screeners are better than they are at detecting concealed weapons, terrorists can exploit this gaping hole in our security to kill thousands more people someday.

There should be no mystery as to what it takes to improve screener performance significantly. The recommendations that my former office made four years ago remain as valid today as they were then. Screeners need to be trained regularly and stringently, under conditions that approximate real world ones as closely as possible. Screeners whose performance is consistently sub-par must ultimately be fired. Supervisors must be evaluated on the basis of their success or failure in training their teams. Supervisors whose teams consistently perform in a sub-par fashion must ultimately be fired. And, technologies like "backscatter" that can see through clothing and spot concealed guns and knives, and "multi-view x-ray" technology that automatically rotates bags in a three- dimensional fashion, ultimately revealing concealed weapons, must be moved beyond the testing and pilot phase to wide deployment. It may be impossible to spot concealed weapons 100% of the time, but through better training, closer supervision, and more widely deployed sophisticated technology, we can come as close to 100% detection rate as is humanly and technically possible.

All these many years after 9/11, we have still failed to grasp that airport screeners are our very last line of defense before another group of hijackers attempt to board planes and carry out another devastating terror attack on our homeland. TSA's compromise of screener testing endangers the security of the nation, and everyone responsible for this particular compromise, and any others that may have occurred over the years, should be subjected to the maximum penalty the law allows.

Chairman THOMPSON. I thank all the witnesses for their testimony. I will remind each member that he or she will have 5 minutes to question the panel. I now recognize myself for questions.

Assistant Secretary Hawley, as I mentioned in my opening statement today, TSA has been very cooperative with the staff investigating this issue. I would like to get your word that going forward, TSA will continue to be cooperative in providing documents as well as making the necessary individuals available to committee staff to talk to.

Mr. HAWLEY. We absolutely will be cooperative. I think that is a blanket statement forever, and we have worked with the committee on a variety of sensitive issues and will continue to do so to get whatever issues there are ventilated and show the truth.

Chairman THOMPSON. Thank you, and I appreciate that.

The other issue I want to kind of talk briefly about is you indicated that this e-mail was recalled. Will you provide the committee with a copy of the e-mail recalling the earlier e-mail?

Mr. HAWLEY. When the inspector general finishes the investigation, they will issue a full report with whatever they find in it. So I would prefer to let the inspector general work until that effort is complete and then, as you say, let the chips fall where they may. So I don't have any issue with withholding anything that is relevant to this.

Chairman THOMPSON. Well, you just said you will provide us with any documents.

Mr. HAWLEY. Yeah.

Chairman THOMPSON. I mean, if you have this e-mail you referenced in your opening statement, it is just a matter of providing it to the committee.

Mr. HAWLEY. It will go through the IG. The IG has its investigation and they will issue the report. I am just reporting to you—

Chairman THOMPSON. So you are qualifying your earlier statement.

Mr. HAWLEY. No, not at all, not at all. I haven't myself touched the document, so I don't want to say I will produce X document. But what I just described to you was what I know to be the case, and then that the inspector general independently is assessing that in the report.

Chairman THOMPSON. So do I assume from the recalling of this e-mail that somebody in TSA knew that this e-mail had been sent?

Mr. HAWLEY. Well, Mike Restovich knew when it was sent when he received it, and said "What's this?" and then went back to the office and said, "Pull it back." And that was 13 minutes from when it was sent by another individual.

Chairman THOMPSON. Just for the record, Mr. Assistant Secretary, when did you see this e-mail?

Mr. HAWLEY. I saw it the other—a week or so ago when the press release went out.

Chairman THOMPSON. So you had no prior knowledge of it?

Mr. HAWLEY. I had no prior knowledge of it.

Chairman THOMPSON. Do you think that the NETHUB system that sent out this notification that the covert testing was taking place was an appropriate use of the NETHUB system?

Mr. HAWLEY. Well, the e-mail, in my judgment and with hindsight and plenty of time, clearly should not have gone out. The individual who sent it out, sent it out believing that it was time-sensitive. And it came the day after the shooting in the Cleveland airport where we have stood up our incident management system to immediately alert all FSDs. If somethingis happening in one airport, they need to be alert everywhere to be on their toes. There was some suspicious elements from this e-mail, specifically the DOT FAA testing, because as you know, DOT and FAA do not do unannounced covert testing with TSA. So it was a good-faith, perhaps, mistake in judgment to send it out. But as soon as it happened it was recalled by senior leadership.

Chairman THOMPSON. Has anyone been disciplined because of this e-mail?

Mr. HAWLEY. No, sir. Well, I think we are going to wait for the investigation to be complete until we find out what the story is.

Chairman THOMPSON. Who sent it out?

Mr. HAWLEY. An individual—I am not comfortable saying the name. I will be happy to provide it to the committee after the process.

Chairman THOMPSON. If you had seen this e-mail yourself, Mr. Hawley, what would you have said?

Mr. HAWLEY. Well, I—with hindsight I would say—well, actually the issue gets to operational communications. And operational communications need to be go out of TSOC; so NETHUB is not meant to be instant operational, it is meant for instant informational. Operational stuff goes through TSOC.

So I would have said if this is true, get it out to TSOC. If we have probes, we need to know about it and find out.

Chairman THOMPSON. Mr. Kutz, do you think it is advisable to notify any operation that covert testing will be going on?

Mr. KUTZ. Our practice is not to do so, so we believe the most realistic test is not to notify in advance. And I think that the question would be, is if you did notify in advance, would the results be different? And our belief is that they would be. It doesn't mean that a blue team test, as I described in my opening statement, doesn't have value. Our information technology people test government computer systems security using a blue team approach. And we do it so that we don't bring down a system and cause millions of dollars of damage. So in that particular case, we don't. But the way we do covert testing with cover teams, we believe it is safe and we believe that not notifying is the best way to do it.

Chairman THOMPSON. Thank you.

I must say, Mr. Hawley, I am a little troubled that for a long time we were told that basically no notifications of any covert testing had ever gone out. And then we hear today that a recall of an earlier notification had gone out. So that is a little troubling, I know, to me as Chair of the committee.

I now yield to the gentleman from California for his questions.

Mr. LUNGREN. Thank you very much. Mr. Hawley, I am trying to understand this. Even though the e-mail said it came from Mike Restovich, is what you are telling us it did not come from him?

Mr. HAWLEY. That is correct. It came from the Office of NETHUB. He was the head of the office, and they issued bulletins sometimes without him actually authoring them.

Mr. LUNGREN. So it is your information and your testimony at this time is that he did not author this nor know about it when it went out; is that right?

Mr. HAWLEY. That is correct.

Mr. LUNGREN. So that then he was made aware of it by reading it; is that correct?

Mr. HAWLEY. Correct, after it had gone out.

Mr. LUNGREN. And when he looked at it, in his mind as you understand it, he thought it was a mistake and so then he recalled it; is that what you are saying?

Mr. HAWLEY. Yes, sir.

Mr. LUNGREN. And what I'm also trying to figure out is the FAA/DOT reference here. Is what you are saying the person who sent it out, who is not identified at this time, had some suspicions about somebody testing the system because it said FAA and DOT and they are not authorized to do this? I am just trying to see if this is what the story is. And, therefore, he thought it was suspicious. And because you had had an experience just the day before, he sent this out in this form, which now we look at and it looks suspicious to us from the standpoint of being a covert operation being revealed to the people who are supposed to be tested; is that right?

Mr. HAWLEY. That is right.

Mr. LUNGREN. That is what you are telling us.

Mr. HAWLEY. Correct.

Mr. LUNGREN. OK, I will await the findings of the inspector general on that.

Now, Mr. Ervin said that this is exceedingly important because the screeners are our last defense against people trying to penetrate. If that is true, there are other layers, is that correct, when we are talking about an operation here?

Mr. HAWLEY. That is correct. And the checkpoint is not the last line of defense.

Mr. LUNGREN. Do you test those other layers?

Mr. HAWLEY. Yes, sir.

Mr. LUNGREN. Are they covertly tested as well?

Mr. HAWLEY. Well, they are both covert as well open testing.

Mr. LUNGREN. Now, Mr. Ervin said that his office recommended several years ago that screeners be trained regularly and stringently under conditions that approximate real-world ones as closely as possible, and then said this is not being done now.

Mr. HAWLEY. That would be incorrect.

Mr. LUNGREN. Well, how do you tell.

Mr. HAWLEY. Because they do 2,500 actual covert tests using bomb parts every single day.

Mr. LUNGREN. But he said real-world ones, as closely as possible.

Mr. HAWLEY. So that is a mistake in statement.

Mr. LUNGREN. No, what I mean is how do you mean that what you are doing is real-world?

Mr. HAWLEY. It uses actual bomb component parts from our covert—from our very professionally developed covert testing kit. It uses detonators, it uses simulated explosives. It is the real deal.

Mr. LUNGREN. Mr. Kutz said that what they do when they do their covert operations is they base it on information that is publicly available, if I understand it.

Mr. KUTZ. That is how we do ours; that is correct.

Mr. LUNGREN. Now, do you do that or do you use information you receive as a result of intelligence? And if you do the latter, why? And why would you do that instead of what Mr. Kutz has said?

Mr. HAWLEY. We absolutely use the Intel Community's information to craft our security measures and our tests and we go after the ones when we find out something they may be training to, and then we go test it to see how vulnerable are we to this, and then we adjust the security measures.

Mr. LUNGREN. Now, Mr. Ervin also said in his testimony that screeners and supervisors whose performance is constantly subpar must be fired, and indicated that, I guess, he doesn't believe that is happening.

What, if any, program do you have that evaluates the performance of both screeners and supervisors, and if they are "consistently subpar?" and I would love to have you define that, and Mr. Ervin define what that meant. Have they been fired, are they fired, do we have the processes by which you are allowed to do that, and if you do, have you done it?

Mr. HAWLEY. Yes, yes, to all of the above. The thing that we have added, we have always had the stick, if you fail your certification at the end of the year, you are fired. And that unfortunately has happened a great deal.

We now have a remedial education part of that that allows people to retrain and pass. Our objective is not to get rid of people but to improve our screening. And now we have added bonuses to high performance, so we have a more positive motivation.

Mr. LUNGREN. When you do these covert tests, are they for the purpose of evaluating performance of an individual employee and therefore that becomes part of his or her employment jacket and you can make judgments with respect to employment status on it, or is it a means of training, or is it a little bit of both?

Mr. HAWLEY. It is training, and we do it with teams. We like to have a team effort both in terms of the TSO in front, the X-ray, and the person doing the pat-down or the bag search. So we say it is a team activity and we do it to train.

Mr. LUNGREN. So if I fail and I am a screener and you have come by 10 times in the last month at my station and I failed every time, that is not taken into consideration whether I am doing my job?

Mr. HAWLEY. If the person fails on the job with our job testing, what we try to do is train and improve on what they are doing. Sometimes we are throwing them things that the technology can't detect, and we have some things where it would be unfair to have a punitive aspect to the training. So what we do is we keep the training positive and the testing in a separate category.

Mr. LUNGREN. My time is up, Mr. Chairman, thank you.

Chairman THOMPSON. Thank you very much.

Mr. Ervin, you were referenced a couple of times, so we will give you an opportunity to respond.

Mr. ERVIN. Thank you very much for that, Mr. Chairman. There are just three quick points I would make. With regard to this issue

of whether screeners are the last line of defense, what I said in the statement was that screeners were the last line of defense before another group of hijackers boards airplanes. Certainly cockpit doors, for example, have been hardened since 9/11, some pilots are armed, and both of those things could help to prevent another homeland security attack in exactly the same manner as 9/11. But I was talking about the last line of defense before hijackers board airplanes. There is no further screening of people boarding airplanes after they have passed the checkpoint.

Mr. HAWLEY. That is not correct.

Mr. ERVIN. I was talking about real-world conditions. There are a couple of elements to real-world conditions. One of those elements is the weapons at issue be as sophisticated and as like real-world guns and knives and bombs as possible. The other element of real-world testing is that the test not be compromised and screeners not be alerted beforehand.

And third, by consistently subpar, we can't in an unclassified session talk about particular results at airports, but as I am sure you know, Mr. Lungren, the results have been consistently very poor indeed at airports throughout the country, both Federalized airports and privatized airports since 2003.

Chairman THOMPSON. Thank you very much.

We yield to the gentleman from Washington for 5 minutes, Mr. Dicks.

Mr. DICKS. Mr. Hawley, it sounded to us like you were making a judgment.

Chairman THOMPSON. Your microphone.

Mr. DICKS. Usually I am easily heard, as my colleagues noted.

Mr. Hawley, it sounded as if you were saying that you didn't think there was a problem here. I mean, your statement clearly states that there was a problem, that this should not have happened. Now, would you testify now and tell us that this should not have happened?

Mr. HAWLEY. I was referring to an integrity problem, a cheating problem and not a supervisory control problem. I think there will be some very interesting things that come out of the test. I don't mean to say that is not going to be valuable, but the pieces on the integrity I have to say publicly, because it has been out all over the media, there is stuff in the paper today that is just plain wrong, and it is unfair to the individuals involved and most importantly it is unfair to the TSOs—

Mr. DICKS. You can't be seriously saying that what this individual did wasn't a breach of integrity or lack of—or made a mistake, he made a mistake?

Mr. HAWLEY. Well, making a mistake is different from lack of integrity.

Mr. DICKS. The person who recalled this thing in 13 minutes thought there had been a mistake made.

Mr. HAWLEY. A mistake. I acknowledge we make mistakes frequently, unfortunately. But integrity, we do not have integrity lapses.

Mr. DICKS. You don't think this was an integrity lapse?

Mr. HAWLEY. No, sir, absolutely not.

VerDate Nov 24 2008 12:26 Nov 06, 2009 Jkt 000000 PO 00000 Frm 00031 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-86\48981.TXT HSEC PsN: DIANE

Mr. DICKS. Mr. Ervin, as inspector general would you think this is an integrity lapse?

Mr. ERVIN. Absolutely.

Mr. HAWLEY. He doesn't know the facts.

Mr. ERVIN. Absolutely, Mr. Dicks. I do not understand this apparent claim on Mr. Hawley's part that the rationale for this was that this was improper testing because DOT and the FAA are not authorized to test. It is true, but there is nothing in the e-mail to suggest that. If you read the e-mail on its face, the apparent implication here, it is pretty clear, is that this was intended to alert the screeners so as to improve their performance on the test. It is just obvious. I do not understand the contrary impression of this.

Mr. DICKS. Mr. Kutz, you are an experienced person. Do you think this is a prima facie case of someone making or doing something that was wrong?

Mr. KUTZ. I don't know. I would say that it could impact the integrity of the test. The integrity of the people is a different matter. If someone is notified in advance of a covert test, it clearly affects the integrity of the test, and that would be all I could probably respond to.

Mr. DICKS. Well, it just seems to me that this is a pretty open-and-shut case, that somebody made a mistake. You should not have sent out this e-mail.

Now, Mr. Hawley if you are going to defend this individual, I want to hear your defense of this individual when your statement says exactly the opposite.

Mr. HAWLEY. No. My statement is there is an inspector general investigation going on, let us let it run its course and find out what happened. I acknowledge when I read the e-mail, I looked at it and said "what in the heck is this," which apparently was very similar to the reaction that Mike Restovich had when he saw it back in April 2006.

Mr. DICKS. Right.

Mr. HAWLEY. And then he had it canceled. So here is a difference between do errors occur at TSA? The answer is yes, they do. If the question is, do we cheat on covert tests and is there some kind of integrity issue where management is cheating on tests, the answer: The facts do not bear that out.

Mr. DICKS. Let me ask, do you have any knowledge of any other example of coaching or whatever you want to call it, of letting people know that there might be a test? Have you got any other example that you know of?

Mr. HAWLEY. Yes, I have heard allegations and I have read IG reports from before I came to TSA, but as far as what is going on today, the covert testing is so much a part of the professionalization of our work force and focusing on IEDs, there is to reason—if we are doing 2 million a year, there is just—it's not something that we would go try to mess with. We need this information to stop attacks.

Mr. DICKS. Mr. Ervin, do you think there are other examples of this that you are aware of?

Mr. ERVIN. Absolutely, Mr. Dicks. There is an Office of Inspector General report from August 2007, just months ago, that is talking about an investigation at TSA, an investigation at Jackson Evers

International Airport, and it says that TSA employees at Jackson Evers International Airport provided advanced notice to other TSAs at this airport. This allegation was confirmed.

Now, Mr. Hawley says that this happened before he arrived. This is August 2007, this report. There is also a report that says confirming—

Mr. PERLMUTTER. What was the date?

Mr. ERVIN. This report is August 2007.

Mr. PERLMUTTER. The date of the incident?

Mr. ERVIN. The testing was conducted in 2004.

I think the main issue here is whether there are other instances of compromise of these tests. And there are. There is another instance in San Francisco as well.

Mr. DICKS. Mr. Hawley, I would hope that your position would be that this is unacceptable. I don't think you could hedge on this. The integrity of these tests should not be thwarted by advance knowledge, and you should make it very clear. And I think by trying to defend this, you are undermining the program itself, and I would hope you would reconsider your position.

Mr. HAWLEY. Thank you. I agree with your statement covert testing, if tipped off, undermines the integrity of the whole system and is despicable. And so it is absolutely wrong, knowledgeably tipping off covert testing is wrong.

Mr. DICKS. Thank you. Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you.

I now recognize the gentleman from Florida for 5 minutes, Mr. Bilirakis.

Mr. BILIRAKIS. Thank you, Mr. Chairman.

Mr. Hawley, can you provide me and my constituents any assurances about the sanctity of the covert testing that screeners at some of the Nation's busiest airports such as Tampa, Miami, and Orlando are receiving on a daily basis as you testified?

Mr. HAWLEY. Yes. We have many levels of covert testing that are done in addition to GAO, the inspector general. We have our own Office of Inspection. And they are out there, they have done something over a thousand tests here in the last year. We have a rigorous program of covert testing plus the ones that I mentioned earlier that we do every day at the checkpoint, and it is very professionally done.

We have some different protocols than does GAO, but we have our own protocols that are well understood and they actually drive our security measures. Security measures we have in place today are driven by the results of our testing. So it is a no-kidding issue that we are doing. We get intelligence from the Intelligence Community, we go test it, and we do change our security procedures based on this covert testing.

Mr. BILIRAKIS. In your written testimony you said that TSOs are among the most tested work force in the country, and you just said that again. Testing is one thing, but results are certainly another. Would you please share with us your assessment of screener performance systemwide?

Mr. HAWLEY. Increasingly better, because we keep raising the bar. We used to test previously with what we call the Wiley Coyote bomb, which is a big thing that you can't miss, that you can't pos-

sibly miss. We have now gone to bomb components. We switch from just testing as previously assembled bombs; now we do the tiniest bomb components that we put in, and we continue to raise the bar. So as the grades go up, we keep trying to increase the difficulty, because it is an evolving threat and they are going to keep coming at us with different things. So we have to keep the test up with whatever might be changing.

This is an actual test object. And yes, you can get 80 percent, you can get 90 percent, you darn sure should get 100 percent. But this is not real security testing, it is testing for the purpose, for a good grade perhaps. We use tiny improvised explosive device components that we have, every kind of imaginable configuration that are extremely difficult to test, but, unfortunately, that is the enemy that we face.

Mr. BILIRAKIS. At a recent hearing, the head of the Screener Union testified the media reports about the inability of screeners to detect simulated explosives and bomb components during covert tests are not good indicators of overall screener performance and did not satisfy him that there is a systemwide security problem. Do you agree; is there a systemwide security problem?

Mr. HAWLEY. I think our security is the best in the world. And I think having said that, there are vulnerabilities, we acknowledge that. The question is how do you manage risk against them? How do you go after the attacks that would cause severe damage to an aircraft in the aviation environment? How do you figure out how to stop those first and work your way back? So it is the best in the world, but, yes, there are vulnerabilities and we have to keep moving to stay ahead.

Mr. BILIRAKIS. Mr. Ervin, can you address that as well?

Mr. ERVIN. Well, all I can say to that, sir, is that consistently, report after report, year after year, continues to show that screener performance is dismal, is the only word I can think of. We found that consistently in the tests that we conducted, as I said, at large airports, small airports, Federalized airports, privatized airports, those results were obtained in 2005 as well by other independent investigations.

Last fall at Newark International Airport, 20 out of 22 tests were failed. And of course, there was the USA Today story just a couple weeks ago showing a 75 percent failure rate at Los Angeles airport and a 60 percent failure at Chicago airport. I might mention that there was a 20 percent only failure rate at San Francisco. We don't know why that result was so significantly better than the results at those other two airports. It could, however, be that the reason for that was that that test was compromised at San Francisco airport, because as I said we now know through a DHS Office of Inspector General investigation that an investigation 2 years ago at the San Francisco airport was in fact compromised.

Mr. BILIRAKIS. Mr. Secretary, I want to bring up an important matter to your attention. You may be aware on Monday a teenager in Tampa near my district, Jody Hall, had an apparently unprotected pipeline that resulted in the release of toxic ammonia cloud, the evacuation of almost 4,000 people, and the closure of several schools.

Madam Chair, I would like to brief you on this as well. I want to let you know that I will be contacting TSA about the security of these pipelines, especially in the Tampa Bay area, and the role TSA is playing in their inspection and security. I hope that you will direct the appropriate officials under your direction to take this matter very seriously and respond to the inquiry expeditiously. So if you can get back to me on that, I would appreciate it.

Mr. HAWLEY. Yes.

Mr. BILIRAKIS. If you have a comment on that, I would appreciate that as well.

Mr. HAWLEY. Yes.

Mr. BILIRAKIS. Thank you very much. Thank you very much, Mr. Chairman.

Chairman THOMPSON. Now yield to the gentleman from Oregon for 5 minutes.

Mr. DEFAZIO. Mr. Chairman, I am a little concerned that we seem to be saying that the screeners aren't infinitely better than on 9/11. Mr. Ervin seems to be trying to say that. The fact is on 9/11 we had the lowest paid employees in the airport. It was an entry-level job from which people hoped to move up to McDonald's. It had 200 to 300 percent turnover rate in some airports. They didn't have background checks, some were illegal aliens, some were criminals. And the failure rates were dismal. But the tests, as Mr. Hawley pointed out, were not very sophisticated.

When I came here in 1987 I introduced my first bill on enhancing security, because at that point the test was a fully assembled 45 enclosed in a block of lucite, with no more than three articles of clothing in the carry-on bag, and the failure rate was comparable to what it is today. But today's test would be finding something very, very small, as Mr. Hawley said.

Now where I would agree—and this is where I want to go with the question—is your points about the enhanced technology. I think the people are infinitely better. The tests are much more sophisticated. The threats are incredibly more sophisticated, and they are still working with the same crappy old equipment, 1970's technology. So I think your point here about the multiview X-ray, the Backscatter, which I have been harping on for years and, because of some privacy issues, even though we could, say, ask people to voluntarily go through it and then frisk the others, we haven't deployed these things fully.

Mr. Hawley, where are we on new equipment?

Mr. HAWLEY. On the checkpoint security for carry-on baggage, we have just procured 250 additional so-called AT machines for the checkpoint that are upgradeable, including multiview. They will be continually upgradeable by the software. So we, as you know, have done a number of pilots over the summer. We like the results and put in a buy order for 250 units.

Mr. DEFAZIO. How many machines are there nationwide, though?

Mr. HAWLEY. Oh, probably a 1,000-odd. So we will continue to upgrade the checkpoint technology. On the Backscatter there is another technology that we just started.

Mr. DEFAZIO. Millimeter wave.

Mr. HAWLEY. Millimeter wave and it has been going for a couple weeks in Phoenix, and the acceptance rate from people offered the

chance to go through it is over 93 percent. So we are very, very encouraged at the public reception to it. It has very good security implications and we are looking at possibly deploying it in primary screening, which would be a very big step up for security, and that would be my hope going forward, is we have a combination of millimeter wave of the person and the AT at the checkpoint.

Mr. DEFAZIO. I hope we have that as soon as possible, because I believe that we are asking people to do the impossible with the equipment they have.

I have another issue. There was some talk about the last line of defense is the flight deck door. Do you have authority, Mr. Hawley, to mandate a secure cockpit; i.e. We are now building planes that are going to fly for up to 24 hours, 787 and A380? I was told by Airbus—they apparently were mistaken or something, I would say politely—that all A380's would have secure flight decks. You have crew changes, they would have kitchens, they would have labs, they would have sleeping areas, and this would all be behind a secure facility.

I then went to Boeing and said, I think you ought to match what Airbus is doing here; this would make a lot of sense. Boeing says, Airbus isn't doing that. I went back and Airbus said, oh, yeah, you are right, it is an option. Well, no one is going to buy the damn option because it costs them one or two revenue seats.

The point of vulnerability is I flew across the country yesterday, the pilots came in and out and the flight attendants stood behind the cart, but then there was when the FAA inspector came out to BS with the flight attendant for half an hour, you know; three times that flight deck door was opened in one flight.

Now, in a 24-hour flight with an A380 or 787, the crew will be in the back. They will walk all the way through the plane and then open the door and go in. This is an extraordinary point of vulnerability. Why can't we mandate that? Do you have the authority to mandate that?

Mr. HAWLEY. We do, but share it with the FAA, because any changes to the area frame have to get safety OK from the FAA. Your point is well taken. With the FAA we already, as you know, have the cockpit door physical requirements, but you put your finger on exactly the issue, which is the security measures in place when the door is opened in flight. And that is an area where further regulation could occur, should that be required.

Mr. DEFAZIO. Well, what would it take to say we are about to build a new generation of planes, and we are going to say that any one of those extended flight planes, newly manufactured, is going to land or take off in the United States, and we will have to have a secure flight deck? The crews will have to be locked in when we take off, and they are not coming out and no one is going in until that plane lands. And they will have everything they need up there to sustain themselves except the company of the flight attendants.

Chairman THOMPSON. The gentleman's time has expired. You can go ahead and answer the question.

Mr. HAWLEY. I would have to take that back to go look at it. I appreciate your concern.

Mr. DEFAZIO. I would hope the Chairman would join me in that, because I have run into a dead-end with the Aviation Committee.

VerDate Nov 24 2008 12:26 Nov 06, 2009 Jkt 000000 PO 00000 Frm 00036 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-86\48981.TXT HSEC PsN: DIANE

We might have to take one or two seats out, or something out of these planes. These planes are going to be unbelievable targets; 700, 800 people in one plane, what a target.

Thank you, Mr. Chairman.

Chairman THOMPSON. Thank you, I would be more than happy to join you.

Gentleman from New York 5 minutes, Mr. King.

Mr. KING. Thank you Mr. Chairman. I want to thank Mr. Lungren for filling in for me at the beginning. I couldn't be here. I want to thank the Chairman for calling the meeting, and I will be yielding most of my time to Mr. Lungren.

Mr. Hawley, I would like to ask you for one point of clarification. Mr. Ervin mentioned the fact that in the IG report, the preliminary report that came out in August of 07, it said that covert testing was compromised at the airport in Mississippi. But as I read it, did it not also say the finding was TSA's Office of Inspection did not provide the advance notice, that it may have come from employees?

While it is to me reprehensible that that happened, to me there are any number of times in law enforcement when you find someone at the ground level will tip somebody off. It obviously has to be stopped. But I think to imply that somehow that was sanctioned or was encouraged by TSA is wrong, but I ask you for your comments on that.

Mr. HAWLEY. It was 3–1/2 years ago, and I think the trail has gone cold, and I don't know exactly what happened. What is important to me is if I can get information on someone who acted improperly, I can take action against that person and will take action against that person.

What I can't do is, there was discussion in the airport about it 3–1/ years ago. That unfortunately doesn't give me room to go attack. But I think as the Chairman is aware, we have made major changes at Jackson to increase not only the work environment, but the total package there in Jackson. So I am highly confident of the security in place at Jackson today.

Mr. KING. I yield the balance of my time to Mr. Lungren.

Mr. LUNGREN. Mr. Ervin, you talked about the episodes that have occurred in the past and that, therefore, they constitute a pattern. When I practiced law, I had to prove pattern and practice at times; and it took more than just a couple out of, you know, 500 or 450 different airports and tens of thousands of actual tests. Do you think your comment is a little harsh?

And I don't want to undercut anything about anybody who did something to undercut the integrity of the testing. But you have made a broad statement of a pattern, and I think you pointed to three or four. And we are talking over a number of years and we are talking about thousands of employees and thousands of tests and 408 or 450 airports. Do you still think that is a pattern?

Mr. ERVIN. Yes, sir, I do. I do think it is a pattern. And I think we can quibble about what constitutes a pattern, but to me a pattern is more than one instance. Three or four instances over a period of time, particularly when—and this gets back to the point that Mr. DeFazio was making—we consistently see year after year that screener performance is very, very poor. So, yes, I do think it is a pattern.

Mr. LUNGREN. OK. Let me ask Mr. Hawley. You have heard the comments that we have had dismal performance year after year after year. That would suggest to me we have seen no improvement. Mr. DeFazio said we have got higher-paid employees, we do more testing, more sophisticated testing. I would hope that that would bear some fruit.

Mr. HAWLEY. Absolutely. And the additional layers of security are a critical piece of this.

Mr. LUNGREN. Let me ask a question about that.

Mr. HAWLEY. Yeah.

Mr. LUNGREN. I have read and visited Israel; and they talk about behavioral inspection, observing people who are there. We are very concerned about profiling and so forth, and I understand that legitimate concern. But, on the other hand, there is something to be said about having a layer of defense that does that. And I don't know if you are allowed to talk about that, but, in general terms, do we do that and is that a part of the layered approach?

Mr. HAWLEY. Yes, very definitely. And we do it in a way that is documentable so that it is not based upon racial profiling or ethnic or anything like that. It is on observable behavior. It is highly successful. We now are doing it throughout the country, and it is the best way to get at somebody who is not bringing a prohibited item, who is doing surveillance or a dry run. You can pick them off with the behavior piece, and that is a highly successful method that we use.

And the President sent up a budget amendment this week for $163 million. Part of that is to expand the behavior detection program to all the major airports for a sizable proportion—

Mr. LUNGREN. I only have 20 seconds left. Let me just ask you this. When you do covert testing, planning, and execution, who in TSA is aware of it and what procedures do you have to make sure the information is not disseminated to those who shouldn't know it?

Mr. HAWLEY. Very limited group. The Office of Inspection does our covert testing and informs the leadership of our Security Operations Group generally, and then at the time that they are doing the testing at the airport they will inform the FSD and the local police for safety reasons.

Chairman THOMPSON. Thank you very much.

We yield 5 minutes to the gentlelady from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Let me thank you, Mr. Chairman; and you are very right to hold this hearing.

I look forward to joining Mr. DeFazio I think on a very pointed line of questioning that is somewhat different from the hearing but focuses on the crucialness of security and the conflict of jurisdiction as relates to the FAA. So I hope there is a wake-up call, frankly, on us working together on this.

And for the record, Mr. Hawley, I would like to join Mr. Bilirakis in getting a response back on that issue that he mentioned in Florida.

Let me try to frame this as a life-or-death matter. Maybe we could focus on the fact that one error in any form of Homeland Security may result in the loss of hundreds, thousands of lives; and

I think that is where we need to focus the inquiry made to you. I appreciate you defending or recognizing there are hardworking front liners, TSA screeners every day going to work. But there is a problem with training.

And Mr. Kutz, let me not ignore you. But I appreciate your testimony, and I think you have laid the framework how vital these covert testing procedures are and how the integrity of that is crucial to your work. So I thank you, and I won't really query you because I want to get the two gentlemen off to the side of you.

I think the problem, Secretary Hawley, is that you never knew what happened. We knew that when we formed the Department of Homeland Security that we had a big elephant to deal with, if I might use that metaphor. But we didn't want bigness to get in the way of security. The fact that you were not knowledgeable about this e-mail is already a fractured part of the structure of this particular department. The other part of it is that Secretary Chertoff certainly did not seem to be aware of it. So let me pose these questions.

And might I say to my—and I will say—good friend, Mr. Ervin, it is clear that your unceremonious departure, your unfortunate departure was one of the Achilles heels of Homeland Security. Being told the truth, they asked the person who tells the truth to depart; and that goes right to the life-or-death matters that we deal with in trying to secure America.

So let me find out whether or not you ever received any documentation of that message being recalled. Where is the data that shows the recall messages? I think we don't have them. And do you have that data that shows these messages were recalled, Mr. Hawley?

Mr. HAWLEY. That is a piece that the Inspector General is doing. As you know, when the investigation comes in, they go after hard drives, they go after systems, and then they take them for their testing. So they are working on that piece. And if there is exculpatory evidence it will be provided.

Ms. JACKSON LEE. We want those as quickly as possible. I know that you are using the IG.

The other question is, how quickly and why did Mr. Restovich not, if you will, notify you? That is a break in the system, as far as I am concerned. You said you just heard about it through a news report. Mr. Restovich allegedly withdrew it, as you tell me that he did, and there is someone who actually wrote it, and therefore there was a break in the chain of command. Why did you not receive the information that that e-mail had been issued?

Mr. HAWLEY. I can speculate. Mike identified a problem, solved it. And things move very fast at—

Ms. JACKSON LEE. Tell Mike that that is not, I think, a line of command that is responsible that the committee would like to see. Because you are in fact the commander, the chief of that area; and I think it is important for you to know that.

I don't want a response, but I am not very happy with that break in the system.

Let me quickly move to Mr. Ervin, and I have one for you. What I would like to see, of course, is that there be a chain of command on these security issues and, frankly, believe that Secretary

Chertoff should also be involved, Secretary Hawley, on this point. I think there is something to sending out a notice saying "be on your toes".

The problem I have with this e-mail is that it specifically points out the actions of the covert actors, Chinese or Asian. This is what they are going to do.

Mr. Ervin, let me go to you on this point. You are absolutely right. We have fought and fought for training. And I think maybe it will be legislation, maybe it will be money, but we give $40 billion to the Department of Homeland Security and about $5 billion to aviation security. What can we do? How hard a foot do we have to put down on this training—and stringent training, if you will—in terms of the TSA screening? I don't want to yield to the fact that they are not educated, that they can't be trained. What does the Department need to do?

Mr. ERVIN. Well, Ms. Jackson Lee, it is very, very clear there needs to be regular training on a consistent basis; and then the screeners need to be held can to account if their performance on a consistent basis, as I said, is subpar.

There is no question but that the training, the testing is more sophisticated now than it was in 2002, 2001. I never disputed that. The issue, though, is, as I say consistently, if you look at the classified reports of the specific results at airports throughout the country of the thousands of tests, tens of thousands of tests over the years that have been conducted by these independent Office of Inspector General, the GAO and TSA itself, you will see that there has not been any appreciable change in screener performance.

And, by the way, I might add that I have yet to hear a convincing explanation as to exactly what the mistake was, if there is an acknowledgment that there was a mistake. And if in fact this message was recalled, why was it recalled?

It is pretty clear to me that the reason that it is deemed to be a mistake and the reason it was recalled is it was pretty clear that it was intended to tip off the screeners. The concern was that this was going to get out to the public, as it clearly has done, and to embarrass TSA. I have yet to hear an explanation otherwise.

Ms. JACKSON LEE. My time is up, but let me just say that one pattern for me is devastating, because that could result in loss of life. Secretary Hawley, I really want to work with you on the training aspect. It might have been well-intentioned to generally notify that something is about, be on your toes, but I think the specifics of this e-mail is a question that raises to a higher level, including yourself and Secretary Chertoff.

And I thank you. I yield back.

Chairman THOMPSON. Thank you very much.

The gentleman from Pennsylvania, Mr. Dent, for 5 minutes.

Mr. DENT. Thank you, Mr. Chairman.

Mr. Hawley, in followup to what Mr. Lungren had been talking about with respect to who has knowledge of the planning and execution of these covert tests, let me take it just a little step further. Has TSA ever taken any disciplinary action against any TSA employees who are involved in giving advanced notice of some kind of a prior covert testing to other TSA employees or TSOs?

Mr. HAWLEY. I am aware of an incident that was just resolved in Jackson, Mississippi, where an individual, after a covert test, described the way that the test was done to other TSOs and received discipline for that. And I believe that on—I am not personally familiar with all the disciplinary actions before I came to TSA, but that would be one I am aware of.

Mr. DENT. When would you ordinarily believe that disciplinary action—some kind of disciplinary action would be warranted?

Mr. HAWLEY. Certainly anything that has to do with integrity is an automatic. We have a very disciplined program for employee discipline that goes through a process that is fair and meticulously investigated. I am not part of that. It is part of our career management to go through what we call disciplinary review, and they dispose of those cases.

Mr. DENT. Thank you, Mr. Hawley.

And to Mr. Kutz, what sort of followup will the GAO be doing to its 2006 review of the covert security vulnerability testing in airports?

Mr. KUTZ. Well, when we issue reports like that, we look to see what kind of actions—

Chairman THOMPSON. I think you might need to turn on your mike. Is it on?

Mr. KUTZ. It is on, yes. I will move it closer.

Chairman THOMPSON. OK.

Mr. KUTZ. We always do followup with respect to testing we do to determine what kind of actions have been taken. I think Mr. Hawley has said that he has used our testing similar to his own testing to try to improve operations, including the human capital processes and technology. So just because we are independent of TSA doesn't mean that he can't use our operations in the same manner he uses his own testing.

Mr. DENT. Can I also ask, too, what is your opinion of TSA's Aviation Screening Assessment Program, or ASAP, which began in April 2007 that greatly expands TSA's internal covert testing programs and performs numerous daily tests?

Mr. KUTZ. Well, we support TSA's covert testing programs, whether it be the OI or any other ones that they do, along with the IG's testing. I believe that the use of covert testing or even blue team testing—we are here talking about whether something is covert. In a pure sense, red team covert testing versus if someone's tipped off in advance, the testing can still be valuable even if people are tipped off in advance. And so I think any type of testing that is being done is constructive in this environment.

Mr. DENT. OK. Thanks.

I will yield back, Mr. Chairman. Thank you.

Chairman THOMPSON. Thank you very much.

We now yield to the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. Chairman, it has been said there is beauty in truth; and Scripture tells us that if you know the truth, the truth will set you free. I really am interested in the truth today. So if I may, Mr. Chairman, may I approach the witness, Mr. Hawley? I have something I would like to present to him.

Chairman THOMPSON. Please. Five minutes.

Mr. GREEN. I understand. I just want to make sure, Mr. Chairman, that Mr. Hawley and I are talking about the same memo. Mr. Hawley, is this the e-mail that we have been referencing this morning?

Mr. HAWLEY. It appears it is, yes.

Mr. GREEN. And, Mr. Hawley, is it true that there was some sort of test that was taking place that this e-mail references?

Mr. HAWLEY. There were IG tests going on at the same time. This was—I should tell you—

Mr. GREEN. If you would, please, the Chairman has reminded me I only have 5 minutes.

Mr. HAWLEY. Sure.

Mr. GREEN. Is it true that there were tests taking place that were referenced in this e-mail?

Mr. HAWLEY. I don't know. I would assume that—

Mr. GREEN. Mr. Hawley, you came prepared to testify today. Surely you know whether there were tests taking place.

Mr. HAWLEY. No, there were tests in place.

Mr. GREEN. All right.

Mr. HAWLEY. I do not know the origin of the words used in this e-mail, so I can't tell you—

Mr. GREEN. Please now, we don't want to go to the origin of words. Your diction has been superb. It has been superb.

But let us now talk about whether there were tests taking place. And your answer is yes.

Mr. HAWLEY. Correct.

Mr. GREEN. Is it true that the language in that e-mail references some aspects of the tests that were taking place? Without going into the language.

Mr. HAWLEY. I believe they do, although it is ambiguous—

Mr. GREEN. If it is true that there were tests taking place and the language of the e-mail makes reference to the tests, Mr. Hawley, how can you say that there was no cheating? How can you say that there was no tip-off? Because that is what that language references. It references the test, and it tells someone that there was going to be a test. Is this true?

Mr. HAWLEY. Mr. Green—

Mr. GREEN. Is this true?

Mr. HAWLEY. It is—

Mr. GREEN. Is this true?

Mr. HAWLEY. The which?

Mr. GREEN. Is it true that that language references a test that was going to take place?

Mr. HAWLEY. It appears to me, which is why we asked the question.

Mr. GREEN. If that is the case, then why would you come today and talk about integrity of a person? Mr. Hawley, don't you understand that if a person pulls out a gun and he kills me, whether he does it by accident or design I am still dead? We are talking about whether or not there was a tip-off, not whether or not someone did it with malice aforethought. Maybe it was done accidentally. This is about a cover blown and a tip-off. That is the style of this hearing. The Chairman made this transpicuously clear.

The question is, was there cover blown? Was there cover blown, Mr. Hawley?

Mr. HAWLEY. The investigation by the IG will decide that.

Mr. GREEN. Does that memo cause you to conclude that some cover was blown, Mr. Hawley?

Mr. HAWLEY. It causes—

Mr. GREEN. If not, why would you recall it if there was no cover blown?

Mr. HAWLEY. No, I think it is—I looked at this and said, what the heck is going on?

Mr. GREEN. Exactly.

Mr. HAWLEY. I think the purpose—

Mr. GREEN. Why would that memo be recalled if there was no cover blown?

Mr. HAWLEY. Because the individual who sent it out did not know the covert testing. He looked in his e-mail, and it came from a credible source—

Mr. GREEN. Whether he had knowledge or not, if what is contained in it is true, it doesn't matter whether he had actual knowledge. Maybe he heard it third hand. Maybe it was not primary, secondary, or tertiary or quaternary. He heard it, and it went out. The question is, was cover blown?

Mr. HAWLEY. No. This was not an integrity issue. The individuals acted honorably, and they acted—

Mr. GREEN. I am not interested in integrity. I am interested in the consequences. I am interested in what happened. Let us not talk about integrity.

Was cover blown? Was there a test that was referenced? You said there was.

Now, Mr. Hawley, listen now, this is not about trying to dissect words so that we can present an image that is less than truthful. Mr. Hawley, this is about truth. And the truth is there was some cover blown pursuant to that memo that was recalled.

And it should have been recalled, by the way. I think the recalling of it was the appropriate thing to do. But what we don't want to do is come to these hearings and cause the American public to think that they are getting what they are paying for in terms of security and deserve by virtue of what we do here in this country to protect people, we don't want them to think that they are getting it when they are not. The truth is, there is a problem here; and you are not being helpful by causing people to conclude that there was no cover blown with reference to that memo.

Mr. HAWLEY. All I ask is no rush to judgment. There is an investigation going on. Let it complete. But I cannot live with these statements that say there was an integrity problem.

Mr. GREEN. I am not talking about—I have 10 seconds. Listen. If you would divorce yourself from integrity and let us talk about facts. That is what I—that is why I approached you with that memo. I wanted to make sure you and I were talking about the same document.

Let us talk about the facts. There is no question that that memo references actions that were taking place, and there is no question that you had to recall it. Because you knew and should have known—if you didn't know after reading it, you knew or should

have known that that could be a blow of cover. And that is why you recalled it. That is what happened.

Mr. HAWLEY. I will never separate myself from integrity.

Mr. GREEN. I don't ask you to separate yourself from integrity. I just said let us talk about the facts. Because William Cullen Bryant is right, truth crushed to earth shall rise again. And Carlyle was right, no lie can live forever. And Dr. King is right, although the arc of the moral universe is long, it bends toward justice. We are talking about justice, sir.

I yield back.

Mrs. LOWEY [presiding]. Mr. Etheridge.

Mr. ETHERIDGE. Thank you.

Mr. Kutz, your written testimony refers to the 2006 GAO's classified report on covert testing in several airports across the country. Your testimony states that your investigators passed through the checkpoints, quote, without being caught. According to the NBC and ABC reports, GAO tested 21 airports and were successful in sneaking explosives through the checkpoints 21 times. Last month, USA Today reported on the results of the covert testing done by TSA. According to some data that they released, they reported TSA found 80 percent of the fake bombs at San Francisco International Airport. They also found 25 percent of the fake bombs at Los Angeles International Airport and 40 percent at Chicago O'Hare.

While any failure in our Nation's screening portals is unacceptable, they are clearly much better than ones found by GAO. So my question is, do you have any thoughts as to why these were—why there was such a wide discrepancy between these two? And are the differences in the testing methodologies used by TSA and GAO enough to explain the differences?

Mr. KUTZ. We were able to bring, as you mentioned, improvised explosive devices and incendiary devices on board aircraft. I can't discuss the specifics of how we do that.

Mr. ETHERIDGE. I understand that.

Mr. KUTZ. How we test. You understand that. And we did find, as Mr. Hawley has mentioned, which their own testing finds, also, vulnerabilities in various areas. And, again, I can't get more detailed than that.

So how to explain the differences in the tests, I don't know exactly what the tests were that they did, but we certainly concealed, either on our person or carry-on luggage, various types of items that were brought onto aircraft. So that is the kind of testing that they do. And why they would have had a lower rate than we had, I don't know the answer to that.

Mr. ETHERIDGE. Mr. Hawley, TSA's explanation for the continued failure to find these decoy bombs is the tests are very hard. I think you have shared that earlier today. Your spokeswoman reportedly said, and I quote, we want to have higher failure rates because it shows that we are raising the bar and the tests are harder. Now I don't know about other people, but failure rates like this don't give me a whole lot of confidence.

Mr. HAWLEY. Some of those are not accurate.

Mr. ETHERIDGE. Let me finish, and I will tell you a question. Because I hope the terrorists don't look at this and say that, you know, they like their chances. I think we need to have difficulty,

and I think we need to have realistic tests. I think we all can agree with that. However, Transportation Safety Officers—and, you know, they need to be able to pass the test. I understand that. But my question is this. No. 1, do you stand by your spokeswoman's comments? And, No. 2, what steps are being taken to ensure that we really do run realistic tests?

You have talked about that this morning and that TSA is prepared to stop more than 25 percent. Not 40 percent, not even 80 percent, but we have to get to a hundred percent. I think that is critical, and I think we can all agree on that. Because if any of these materials get on an airplane, we are in trouble; and I would be interested in your comment on that.

Mr. HAWLEY. There are a couple points.

One, if you just test one individual layer, that doesn't tell you anything about the system integrity. So what we do is we design the other layers that we put in place to close vulnerabilities that might be present in one other layer. And that is what we are doing here with the document checker, the behavior detection, with all these other programs, are to buttress up vulnerabilities elsewhere.

Mr. ETHERIDGE. Are you saying then that these did not get on the plane?

Mr. HAWLEY. Well, some of them were not tests at all. There is some quibbling with it in the USA Today article. Those weren't referring to tests. That was referring to training.

But the overall thrust of it is that there are vulnerabilities. We learn of them and we fix them by virtue of either training, technology, or adding additional layers. And back on the issue of training, we had 3 million hours of additional training in 2007.

Mr. ETHERIDGE. Let me back to the original point, though. You are saying GAO didn't get all the way to the plane with theirs either?

Mr. HAWLEY. No, on the GAO I am not going to get into the classified—

Mr. ETHERIDGE. I am not asking on the classified. I am just asking, did it get through?

Mr. HAWLEY. Well, I don't believe they actually had explosives. I think there is a lot of complexity to the tests. I think they proved some interesting things about training and about technology that I welcome, accept, and use. But as far as getting on the plane—

Mr. ETHERIDGE. I see my time has expired, Madam Chair, but I do think this might require a little classified conversation later to get more detail. I yield back.

Mrs. LOWEY. Thank you very much, and we will continue until it is time to vote. Thank you very much.

Mr. Hawley, what is the turnover rate of employees at TSA?

Mr. HAWLEY. Well, for TSOs, it is about 21 percent; and for the headquarters staff it is much, much lower.

Mrs. LOWEY. Do you think—you have been talking a lot about training—that in this particular instance if the workers were operating under better conditions—and I won't go into greater detail, but I would like you to submit that to me in writing, what is the average term that people are staying there? What kind of training have they received in the interim? What kind of salaries are they getting? Is there collective bargaining? I don't believe there is. Is

there a whistle protection act? Maybe one of those people who had seen the e-mails could have responded if they didn't fear retribution. So I would be very interested in the personnel policies.

And with the training that you are providing, how does it keep people working in a more professional way and staying for a longer period of time? If you can provide that to me I would be most appreciative.

Mrs. LOWEY. Second, Mr. Ervin has stated that GAO doesn't alert anybody. GAO's inspections in a whole range of issues, as far as I am concerned, have been quite effective; and I believe you said if there is an incident that would occur they would pounce down.

In your testimony, Mr. Hawley, you say for safety purposes airport law enforcement are notified prior to testing. Do you want to comment on that?

And perhaps, Mr. Ervin, does GAO—am I correct? Did I hear they do not notify anybody? And, therefore, when they are going in they are doing an effective evaluation because they don't have to worry about people being tipped off?

And, by the way, I think Ms. Lee mentioned before, I think, sending out notices every day to remind the people of what they have to do is a good idea. But not alerting them then that inspectors are coming, because that would in my judgment really negate the effectiveness.

Could you comment, Mr. Ervin?

Mr. ERVIN. Sure, Ms. Lowey, of course, GAO can speak for itself, but I just confirmed with Mr. Kutz before the hearing began that it is GAO's practice not to inform anybody before they begin their tests. And certainly that is a valid judgment, and it makes the tests less likely to be compromised.

When I was the Inspector General at DHS—and my understanding is this practice continues today—there is notification, but it is to very small numbers of people, I believe just the FSD, and only minutes before the testing actually takes place. And that is done so as, on the one hand, to protect the screeners and everybody else from being killed actually in extremis or from having a costly evacuation of the airport simply because of a test. But it is done, as I say, just minutes before so as to minimize the possibility of compromise. That is the balance that we struck there.

Mrs. LOWEY. Mr. Hawley?

Mr. HAWLEY. We have a difference of opinion, and there is a tradeoff. With the no-notice tests, they don't use actual bomb components that have explosive residue on them. So we get tremendous value out of using the actual components with the actual explosive residue. That will test—if we are after a particular kind of attack, we will be able to fine-tune exactly on the basis of that. So what the GAO gains by no notice there is a downside that you don't get to use the real stuff. So the flip side is that we do notice because of security concerns, as Mr. Ervin mentioned.

Mr. KUTZ. Could I just comment, too?

Mrs. LOWEY. Certainly.

Mr. KUTZ. When I say "real stuff", we don't use explosives, we use improvised explosives. So these are things available in grocery stores, for example, those types of things.

But with respect to the cover team, I mean—and, again, his position is with what their protocols are they would notify law enforcement. We simply have a cover team that serves a similar purpose, that if someone does get caught doing a covert test it is supposed to defuse the situation so that there isn't a security concern.

So that is how we have had instances before where we have been caught in our testing, and it simply defuses the situation having a cover team right there to say this is GAO, and this is a test.

Mrs. LOWEY. I thank you very much.

Mr. Hawley, there clearly seems to be a difference of opinion on this; and to make this effective I think we should have further discussion on how we can be most effective. Because, frankly, as a New Yorker, I am very concerned about the fact that we are perhaps not training our workers as effectively as we could; and, in fact, I am very concerned about the attrition rate. And if we had people in place for longer periods of time and did provide whistleblower protection perhaps this kind of an incident could be avoided.

And in the 21 seconds, the committee informs me, and I see this list of e-mails, and if we are talking about integrity, it seems very strange that there is a whole list of 37 e-mails, but the recalled e-mail is not included. Now it may be a minor issue. Because, frankly, in my judgment is once the e-mail went out the whole recall is just kind of self-defense, but it really doesn't accomplish anything.

So the issue of worker training, what are we doing to make sure our force is as experienced as we can, whistleblower protection to make sure if someone finds something out they will have, without fear of retribution, the responsibility to report to somebody.

And it is still strange to me that Mr. Restovich kept this all to himself and he didn't think it was important enough and that it wasn't compromising the inspection to tell you about it.

But my time is up. I think are we going to recess? We will recess for a series of four votes. We will reconvene immediately after the last vote, about 30 minutes or so.

There have been many issues that have been raised, and I do hope we can have further discussion. Thank you very much.

[recess.]

Chairman THOMPSON [presiding]. We would like to start our meeting back.

Mr. Pascrell, before I call on you for your 5 minutes, I understand, Mr. Hawley, you want to make a clarification of some previous testimony?

Mr. HAWLEY. Yes. It was related to our exchange about the recall of the e-mail we have in question. You had inquired whether TSA would be forthcoming in providing the committee with such as it has. And the answer is yes. We will work with your staff to, you know, abide by any applicable rules of ethics and good form that would apply with the IG, but I want to be unequivocal in saying we are fully supportive of this investigation.

Chairman THOMPSON. Thank you very much.

Mr. Pascrell for 5 minutes.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Chairman, I just wanted to clarify something that the Secretary mentioned last time he was here concerning whistleblowers. I interpreted what you said as a commitment. Would you just very

briefly tell us that commitment again and where we are about whistleblowing—

Mr. HAWLEY. Yes, sir.

Mr. PASCRELL [continuing]. With screeners who are in the law, as you know?

Mr. HAWLEY. Yes, sir. Very much related to this hearing today is the integrity of the whole process, which includes whistleblowing protection, that we have in place whistleblowing protection. But you and other members have suggested that we go into the formal process for the rest of the government. We are looking at that, and I expect that we will have—that we will get to that point with that solution that we will implement.

Mr. PASCRELL. I think this is going to be a giant step if you do what you say you are doing.

Mr. HAWLEY. We will find out.

Mr. PASCRELL. Second, I would ask you to give serious consideration again, as I have talked to the Secretary Chertoff about problems, having enough screeners; second, them being properly trained. And we have a better chance of fulfilling our mission if we hire former law enforcement officers who are trained to study behavior, eye, facial expressions and everything else. That is my second suggestion.

Mr. HAWLEY. Thank you, sir.

Mr. PASCRELL. In 2003, the President of the United States in his State of the Union address said the following, Mr. Hawley: It would take—in talking about Homeland Security—it would take just one vial, one canister, one crate slipped into this country to bring a day of horror like none we have ever, ever known. We will do everything in our power to make sure that that day never comes.

I want to remind the Department about what the President said and what I thought was a pretty good speech, although I didn't agree with much of it. That is beside the point.

These are troubling times here. We are trying to get to the truth. You know, Mr. Hawley, the memo that we are referring to. You just made mention of it again. My first question is, did anyone else—have you ever seen a notification like this before?

Mr. HAWLEY. No.

Mr. PASCRELL. You have never seen a notification like the one that you just—the Congressman Green showed you earlier and that you just referenced at the beginning of my questioning?

Mr. HAWLEY. That is correct.

Mr. PASCRELL. Never seen that. Now Mr. Restovich's name is on here. Apparently, he never saw it before it went out?

Mr. HAWLEY. Correct. That is my understanding.

Mr. PASCRELL. He never saw it?

Mr. HAWLEY. I would like to say that the Inspector General has his own investigation that will be the definitive one. From what I—

Mr. PASCRELL. So it may be that whoever sent this out with Mr. Restovich's name on it maybe asked Mr. Restovich whether he should or shouldn't. We just don't know. All Mr. Restovich is saying is that he didn't send it out. That doesn't mean he didn't write it.

Mr. HAWLEY. Well, we will wait for the Inspector General. I believe with everything I know Mr. Restovich had no knowledge of this e-mail until after it had been sent.

Mr. PASCRELL. And I take exception—it looks like—if you read this carefully, it looks like there has been others before this. It is just too smooth. It didn't come out of the air. It wasn't invented on that morning.

Mr. HAWLEY. May I respond to that?

Mr. PASCRELL. Sure.

Mr. HAWLEY. It is a cut-and-paste job. What happened is the individual who did send it out saw that, saw the anomaly with the DOT/FAA, was concerned that it might be an al-Qa'ida probe using false credentials, because there is no FAA/DOT allowable instant testing, and was concerned that we would be missing moments. And as you reference the President's speech, it is all about not letting an attack happen, and it is all about getting the information to the people who can do something about it. And in his belief he thought he was doing the right thing to get information out there, with the consequence being—

Mr. PASCRELL. Apparently, he thought he had the power to do this, whoever sent it out.

Mr. HAWLEY. Well, I want of all of our officers, if they feel there is a danger, to get the information to the people who can use it and stop an attack in process. And that is pretty hard to criticize.

Mr. PASCRELL. I have to take exception with you, Mr. Secretary, about in your testimony earlier you talked about an incident that happened in Cleveland the day before. Yes, an incident happened, but if you want me and this committee to believe that that is one of the reasons why this was sent out, I find that as a stretch at best.

Mr. HAWLEY. May I respond to that?

Mr. PASCRELL. I am not asking a question. You can respond to it when I ask a question.

Mr. HAWLEY. Sure.

Mr. PASCRELL. The Bush administration promised us a Homeland Security Department and a transportation administration that could secure our skies. Yet after all this time the greatest assurance that the American public can take in their own security when flying is the knowledge of how much hair gel they can carry on board with them.

We have talked ad nauseam about the critical role of screeners in aviation security, and yet we know that TSA screeners likely have the lowest morale of any group. They have got the lowest morale in the Department. They have got the lowest morale in the entire government, Homeland Security. That is pretty, pretty interesting.

And who could possibly blame them? We asked that they be the last line of defense to prevent another 9/11 style attack, and yet this Department has done everything possible I think before you got there, after you got there to demoralize them.

We need to listen to them. They are on the front lines. Not me, not you. Their supervisors give them a deaf ear. And I hear this all over.

Now, you may have evidence to the contrary. I have never seen it. Instead of empowering them, you refuse to give them this full whistleblower protection that we talked about.

It has been a month now. We need to act on this. Instead of respecting them, you go to extreme lengths to deny them the collective bargaining rights they deserve, chapter two.

So here is my question. Is it any wonder why so many of them feel dejected?

Mr. Hawley, what are you going to do about it to improve the morale of the troops? And don't tell me it is wonderful, because you know it is not.

Mr. HAWLEY. Our work force is fully engaged, and I think you will never have a better test than the morning of August 10th, 2006, when we changed the entire security protocol of the United States instantaneously, and it went smoothly and continued smoothly. And it is because our officers are leaning forward and are committed. We have supported them with career progression, pay raises, better training, better equipment. The reforms that have happened in our personnel system over the last year and a half are astounding. And I would ask anyone to give a fair review of these additional—these matters; and I would ask each Member of Congress, when you go through your airports, talk to your TSOs—

Mr. PASCRELL. I do.

Mr. HAWLEY [continuing]. And find out what the difference is between maybe 2003 and what we have out there protecting our country in 2007. And I am very proud of that work force, and I believe we are locked tight together in the same mission.

Mr. PASCRELL. Mr. Chairman, can I ask two yes or no questions? Quickly?

Chairman THOMPSON. Go ahead.

Mr. PASCRELL. Thank you.

Two quick yes or nos. Do you believe in your heart that the screeners should be deprived of collective bargaining? Yes or no?

Mr. HAWLEY. I believe we have a great work force, and that is a requirement for security.

Mr. PASCRELL. You answered my question.

The second question is this. Is there any desire on the part—has there been any discussion, yes or no, on the discussion of privatizing, going back to rent-a-cop with the screeners? Any discussion about that?

Mr. HAWLEY. We have a system of that, but—we have a system where airports may apply for that. We have not had a system-wide evaluation that would suggest we move in that direction. So I think the answer to that is no.

Chairman THOMPSON. Thank you very much.

We now yield 5 minutes to the gentleman from Colorado, Mr. Perlmutter.

Mr. PERLMUTTER. Thanks, Mr. Chairman.

Just a couple questions about the memo; and Mr. Green, I think, did a good job sort of dissecting the importance of it. But I just want to start kind of at the top. Mr. Hawley, Mr. Ervin, Mr. Kutz, if you would take a look at it. It was sent April 28, 2006, 2:51, to, it seems to me, just about everybody in TSA. Is that right?

Mr. HAWLEY. Many hundreds.

Mr. PERLMUTTER. And then there is a CC to TSNM commercial airlines, TSNM commercial airports. Who is that?

Mr. HAWLEY. It is an internal TSA group called Transportation Sector Management. They deal with the airlines and the airports.

Mr. PERLMUTTER. OK. And so it is still within the TSA—

Mr. HAWLEY. Correct.

Mr. PERLMUTTER [continuing]. Sphere. It isn't the airports themselves. It isn't the airlines themselves.

Mr. HAWLEY. That is correct.

Mr. PERLMUTTER. Then we have James Schear, Earl Morris, Morris McGowan. Mike Restovich is shown as a CC, which kind of lends credence to the fact he didn't send it, because he was getting a CC of it. Who are those folks? And then Susan Tashiro.

Mr. HAWLEY. They are executives in the Office of Security Operations, either Mike Restovich's deputy, general manager in the case of Earl Morris, and Susan Tashiro was assistant to Mike Restovich.

Mr. PERLMUTTER. OK. Now I understand you all have this under investigation and you are going to get to the bottom of how this occurred. But at least a story that has been presented to you is that somebody thought that this was—

You know, the way I am looking at this is you guys do covert testing. In my sort of vernacular as a dad it is a pop quiz. And if you are going to give pop quizzes, hopefully people have had training and education and they can respond to a pop quiz. And in this instance we have several people that give pop quizzes. Somebody else from some other agency may pop in and give a pop quiz, and that is kind of where the IG or the GAO is coming from.

Now, the story that you have at least given to us is that whoever sent this out was concerned that it was a phony pop quiz, and it was being disseminated or being put out there by some group that would like to do us harm. Is that right?

Mr. HAWLEY. That is correct.

Mr. PERLMUTTER. OK. Now—and I will accept that, and your investigation will get down to the bottom of that. But I guess from my point of view is, if that is the case, if it is a probe by some outside organization that is trying to hurt us, that you would get notice of that like ASAP, just as your acronym for this new organization that you, Kip Hawley, and, you know, would be informed immediately. Right? You see what I am saying?

Mr. HAWLEY. Absolutely.

Mr. PERLMUTTER. So if there were an al-Qa'ida probe, as you just mentioned a second ago, that is something I would expect to go right to the top.

Mr. HAWLEY. Exactly.

Mr. PERLMUTTER. But it didn't in this instance.

Mr. HAWLEY. Exactly.

Mr. PERLMUTTER. OK. So Mr. Green's inquiry, really he didn't care whether it was an intentional act or just a mistake. It still happened, and it breached the system. OK. I am concerned, whether it was an intentional act or a mistake, that protocol advising you wasn't followed. That to me is the more damning thing in this.

Mr. HAWLEY. Yes. I think you have raised an excellent issue. And one of the reasons that Mike had a problem with the e-mail was that we have our Transportation Security Operations Center that is the incident management and that our protocol, is all of those things, probes or anything else, goes through TSOC and they

do have immediate contact with me. So NetHub was the wrong place to send out an operational e-mail. So that is one of the learnings that we have from it, of which there are many.

But the individual saw this as a cut-and-paste thing, thought his duty was to get it out immediately, did it in good faith. He was wrong, and it was recalled.

Mr. PERLMUTTER. All right. And I have so many questions. But I will just—OK. Hopefully, this is—whoever sent this and has the—and you said you want your agents, your officers to really, if there is a threat, bang, get out there; and I don't quarrel with that a bit. OK?

We just can't cry wolf too much, but obviously we want to alert people, coordinate, communicate. They have got to be educated enough not to do a cut and paste. I mean, one of the things that is bothering Mr. Green so much, you read this—just the language of the memo is a tip-off. OK? If he was just going to say, hey, I think there is something phony going on here, everybody keep your eyes open, bang, I can, you know, respect that. That isn't what this says.

So my time is up. I got a million other questions, and I will save them for some other time.

Mr. HAWLEY. I don't disagree with that last comment.

Chairman THOMPSON. Thank you very much.

We yield 5 minutes to the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman.

Assistant Secretary Hawley, in your testimony you note that the April 28, 2006, incident is currently under investigation by the DHS Inspector General. However, I am taking from this hearing that this incident may only be one small instance of a far greater problem. Have you begun any investigation into other alleged incidents where covert testing was compromised? Is the current investigation focused solely on the April, 2006, incident or is it probing the fact that this problem seemed to go far deeper than just a one-time incident?

Mr. HAWLEY. We have a system in place. One of them is the whistleblower that Mr. Pascrell referred to, and anytime there is an allegation of any sort in this area it would be actively investigated. I know of no other investigations at this time on this subject other than this one, which is being done by the Inspector General. The other ones that we have mentioned in this hearing, San Francisco and Jackson, were also the subject of IG investigations that have been concluded in San Francisco's and almost concluded in the Jackson.

Ms. CLARKE. And do you find or has there been any analysis of any commonalities in terms of those breaches?

Mr. HAWLEY. Yes. And they are, to my belief, isolated instances. I should say that today every checkpoint, every shift every day has covert testing. So for somebody to say, guess what, you are going to have covert testing on your checkpoints, it happens every day at every checkpoint every shift. So that is why I point out it is just not part of—it doesn't make sense in the TSA context. It would serve no point because, yes, every checkpoint is covert tested every shift.

VerDate Nov 24 2008 12:26 Nov 06, 2009 Jkt 000000 PO 00000 Frm 00052 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-86\48981.TXT HSEC PsN: DIANE

Ms. CLARKE. It just seems to me that for the screeners to sort of reach a point where they are comfortable there has to be a threshold that is met. And it just—there appears to be some serious degradation of the integrity of the professional development of these screeners when you have an incident of this magnitude. How do they differentiate between, you know, what protocol standards are being set versus something that would override it? How do you differentiate that?

Mr. HAWLEY. Well, our officers—I think we have had over the last 2 years exceptional training. We have a hundred bomb appraisal officers deployed in the field that constantly do the testing. We do these ASAP drills and checkpoint drills, and we have built into our staffing package the full boat of training. And in 2007 it was three million hours on top of all of these checkpoint drills that I am talking about. So we understand the importance of the human factor in this is critical.

Ms. CLARKE. Exactly. And I think that is the challenge. At what point does the screener just sort of blow things off?

Mr. HAWLEY. Never. Never. And it is part of keeping—the learning is part of the thinking. And one of the issues we have—and people say this all the time, hey, I got through with this, they let me with that. But what is going to happen if we say we trust you, you are trained, you make a decision and you be accountable for the decision? What you are going to have is people complaining I don't get the answer everywhere. And we affirmatively accept that criticism and say—because, otherwise, we are telling our work force not to think.

And we need to beat al-Qa'ida. With the stuff that they are throwing at us, we need them to think. And there is nobody that has seen more people going through the checkpoints than the officer.

Ms. CLARKE. My question—my next question is for you, Mr. Kutz. Your written testimony references the GAO's 2006 classified report on covert tests of several airports across the country. Your testimony states that your investigators passed through the checkpoints without being caught. Further, NBC and ABC reported that GAO tested 21 airports and was successful sneaking explosives through the checkpoints all 21 times. TSA's success rate, as recently reported in the media, was better than that. Do you believe that GAO's covert testing protocols could result in such a drastic difference in success rates? And just sort of give us a sense of why.

Mr. KUTZ. Not necessarily. I mean, only if the screening lines, again, are tipped off, which, you know, there is an investigation of that about the specifics of what actually is coming. So I don't know if that would account for any differences there. And I don't know the exact testing that they do. They do such a wide variety of testing. Our testing was one type of test at 21 different airports by two testers; and so it was a very narrowly focused test on incendiary devices, including explosive devices.

And, again, I can't account for the difference between what they test because they do such—as Mr. Hawley mentioned, their testing is so extensive and widespread that there could be other factors that result in the differences in the results.

Ms. CLARKE. And could you explain the concept of red team testing?

Mr. KUTZ. Red team where we operate is, again, we are &1 Legislative branch agency, we report to you. We do testing for Members of Congress and committees and subcommittees. Red team for us is we are independent of th. Executive branch agencies that we test. Within GAO, only a few people know, typically, that we are doing a red team test; and no one at the agency is informed in advance of the test.

So, for example, if we did airport testing, we would not tell TSA until after we had tested all of the airports. Once we test all of the airports, our protocols are first to report our results back to the congressional committees, and then we would sit down with Mr. Hawley and/or his people and discuss the details of what we did, what we found; and we would provide any suggestions for improvement based upon what we did.

Ms. CLARKE. Thank you very much, Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you very much.

Mr. Kutz, knowing what you have gleaned from this hearing and that memo, how would you suggest to TSA that we prevent similar occurrences like that or enhance a system to prevent it?

Mr. KUTZ. Well, it is more difficult at TSA. Keep in mind TSA is testing themselves. When we do a test we work for you. We operate on a separate network from TSA. We are absolutely independent, physical location independent, et cetera. So it is easier for us probably to make sure that absolutely no one at TSA knows that a test is happening. So it is difficult. I think internally—and they apparently have other protocols that they follow to try to make sure that people don't know that there is tests in advance. It is going to have to be a TSA-specific protocol. We are in a perfect position to do what I would call a pure covert red team test from where we sit.

Chairman THOMPSON. So in essence you say it is very difficult to kind of police yourself?

Mr. KUTZ. It is hard. You are testing yourself. Mr. Hawley's people are testing themselves constantly, so it is not surprising in some instances people might know in advance there is a test. I am not saying that is what happens, but it wouldn't be as surprising for them to have that happen as if we had it happen. It has never happened since I have led FSI or since I have worked with our former Office of Special Investigations where anyone has been tipped off. And again, I would be surprised if it ever does happen the way we always have it set up.

Chairman THOMPSON. Mr. Hawley, you referenced whistleblower in your statement in reference to Mr. Pascrell. Explain a little bit about the present whistleblower system.

Mr. HAWLEY. We have a system where, if somebody has a whistleblower issue, they are protected. And we use the Office of Special Counsel, which is a separate independent government body to be the appeal authority; and they conduct their investigation. So it is the equivalent of the formal MSPB protection, but it is not identical to it. And what Mr. Pascrell has suggested, and I think is a good idea, is that we should adopt the MSPB formal process so

there is no doubt and there is clarity in the whistleblowing protection. I think that is a fine suggestion.

Chairman THOMPSON. But it is an internal process?

Mr. HAWLEY. No, no, no. It starts as an internal process, and then it goes to the Office of Special Counsel. It is outside. It goes outside. There is an outside, independent review. It is just not the same one as they use for MSPB.

And I think we are vehemently agreeing here. We all want the same thing, which is if somebody sees something that needs to get reported, have a system that protects the public by making it have integrity. And, you know, the feedback here says use this system. I think that is fine.

Chairman THOMPSON. Thank you very much.

Any questions from anyone? Mr. Pascrell?

Mr. PASCRELL. Yeah. Mr. Kutz, how often do you do inspections?

Mr. KUTZ. The covert testing that we do?

Mr. PASCRELL. Yes.

Mr. KUTZ. We have some ongoing right now as we speak. So I would say on a day-to-day basis we have something we are testing.

Mr. PASCRELL. Let us take Newark Airport. I was going to say you take it. Let us take Newark Airport. How frequently in the last 30 days could we have possibly had some covert activity on your part, on the GAO's part at that airport?

Mr. KUTZ. If you are taking airports, I was speaking broader, governmentwide covert testing that we do, not airport specific. So when I said something is going on every day for us, it isn't necessarily TSA. It could be anyone in the government we are testing. So we do very rare airport security testing. That is a very small piece of our broader portfolio. We are not doing any airport testing as I speak today.

Mr. PASCRELL. You are not?

Mr. KUTZ. No.

Mr. PASCRELL. So the only testing going on at the airport is what the Department does?

Mr. KUTZ. Unless the IG is doing it. I understand the IG also does covert testing.

Mr. PASCRELL. So how do we know, how can we conclude that there is testing going on and it is valuable and they are finding out what is going on that is right and wrong in the process of screening, Mr. Kutz?

Mr. KUTZ. There are other people in GAO that look at their covert testing process from a program perspective, and so they do constant reviews. They don't do the actual covert testing like we do. We are an investigative unit. That is what we do. They do performance reviews and constantly are looking at Mr. Hawley's operations, including their covert testing. And so I can tell you that there is extensive covert testing that happens at TSA based upon GAO work.

Mr. PASCRELL. And that operation deals with the actual human being going through the process of being checked, the luggage being checked? So you are a third party that comes in to see if it is being done?

Mr. KUTZ. Yes. I don't think they necessarily will do the covert testing with Mr. Hawley's group.

Mr. PASCRELL. No, I am not saying that.

Mr. KUTZ. But they will review the results and look at the various processes.

Mr. PASCRELL. Do we get those reports from the GAO specifically?

Mr. KUTZ. I don't know if they have gone to your committee. I believe they probably have. They do work for across the government. I believe the answer is yes.

Mr. PASCRELL. I would like to see that.

Mr. KUTZ. And typically they are classified reports.

Chairman THOMPSON. We have one that is in the SCIF right now that—if you would like to look at—

Mr. PASCRELL. I would.

Chairman THOMPSON [continuing]. And I think one is going to be released tomorrow.

Mr. KUTZ. That is correct. One is tomorrow.

Mr. HAWLEY. And I would look forward to working with the committee in a classified session to give a very full discussion on it.

Mr. PASCRELL. I want to see where we were and where we are and where we hope to be—

Mr. HAWLEY. Right.

Mr. PASCRELL [continuing]. So that we know that we have confidence in how we are spending our money. And we want to know whether people are lying to us when they come to testify. We want to know the truth. American people want to know the truth. We are only spokesmen. That is basically what we are.

I don't feel totally comfortable yet, and I am glad that you moved—and that is the first time I heard from anybody from Homeland Security last month, October the 16th, when you testified, that you are heading for a full-fledged whistleblowing program which will include screeners. And it will be an objective program, not something within. And that workers will feel protected if they do come forward and they know they won't feel threatened.

And I think that that is important, and that helps your morale problem, if you have any. You are minimizing the morale problems, but maybe I am talking to the imposters when I go to the airports. I don't know. That isn't the conclusion I would come to.

Thank you.

Chairman THOMPSON. Thank you very much.

I want to thank the witnesses for their valuable testimony and the members for their questions.

I also want to say to Mr. Hawley that we really are looking to a successful conclusion of this e-mail situation. It is a real concern. And there are some other issues with it that we hope through our inquiry you can respond accordingly.

The members of the committee may have additional questions for the witnesses, and we will ask you to respond expeditiously in writing to those questions.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 12:53 p.m., the committee was adjourned.]

VerDate Nov 24 2008 12:26 Nov 06, 2009 Jkt 000000 PO 00000 Frm 00056 Fmt 6633 Sfmt 6011 H:\DOCS\110-HRGS\110-86\48981.TXT HSEC PsN: DIANE