

Rebuilding TSA into a Smarter, Leaner Organization



A Majority Staff Report

Subcommittee on Transportation Security
Committee on Homeland Security
Rep. Mike Rogers (AL-03), Chairman



112th Congress
September 2012

SUMMARY

In the aftermath of the 9/11 terrorist attacks, the Transportation Security Administration (TSA) was created to help restore confidence in aviation security. Congress provided TSA with the flexibility to set policies and procedures for screening people and goods as they moved through our transportation systems. Unfortunately, that flexibility has been exploited by TSA in recent years. Its operations are in many cases costly, counterintuitive, and poorly executed. Despite the reality that we have not endured another successful terrorist attack since 2001, TSA is failing to meet taxpayers' expectations. This report explores why.

During the 112th Congress, the Subcommittee on Transportation Security of the Committee on Homeland Security launched a thorough examination of TSA's operations, rules, and regulations and their impact on job-creating transportation industry stakeholders. This examination included 22 hearings, 15 Member briefings, 7 site visits, and an in-depth review by the Subcommittee's Majority Members and Staff.

This report addresses five central themes and makes the following recommendations to TSA towards rebuilding a smarter, leaner organization:

Advance Risk-Based Security

- Prioritize the harmonization of aviation security standards worldwide
- Adopt a comprehensive plan to mitigate evolving threats
- Expand the use of canine explosives detection assets

Strengthen Privacy Protections

- Enlist the private sector to modernize and, to the extent possible, automate the passenger screening process to reduce pat-downs
- Implement privacy software on all AIT machines
- Sponsor an independent analysis of the potential health impacts of AIT machines

Limit Spending

- Reduce the size of the TSA workforce
- Conduct cost-benefit analyses for all major programs and purchases
- Communicate with industry to avoid setting technology requirements that are unattainable

Create Jobs

- Contract with the private sector to perform screening
- Establish a five-year procurement plan to guide future investments in aviation security technology research and development

Cut Red Tape

- Work with stakeholders to streamline existing security regulations
- Issue final rules for long overdue security programs
- Reform the Prohibited Items List to better reflect evolving threats

TABLE OF CONTENTS

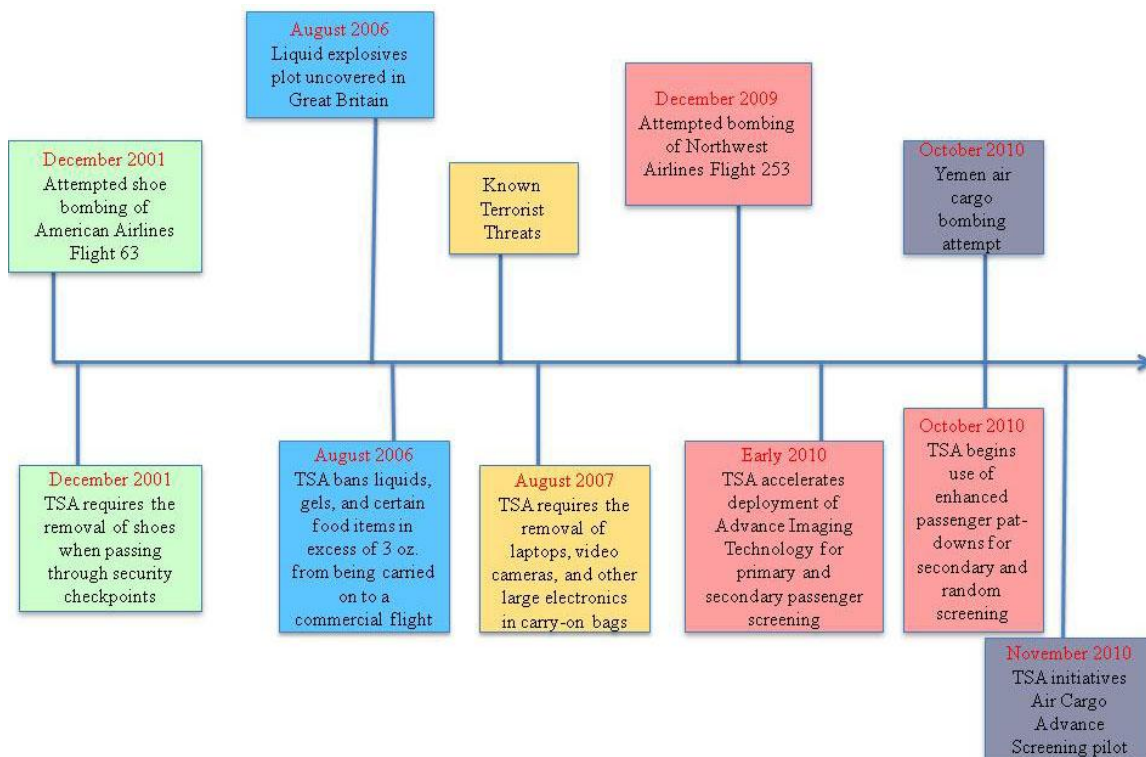
Chapter 1: Refocus on Security Mission	3
The Global Transportation Network	3
Security Breaches Occuring at Airports.....	4
Flight Students Are Not Properly Vetted	5
The Value of Explosives Detection Canine Assets.....	5
Chapter 2: Improve Passenger Experience & Privacy Protections	7
Risk-Based Screening Initiatives	8
Missed Deadline For Revised Military Screening Procedures	9
Weaknesses in Behavior Detection Program	9
Health and Privacy Concerns About Advanced Imaging Technology	10
Chapter 3: Eliminate Wasteful Spending	12
TSA’s Broken Procurement Process.....	12
TSA Personnel Costs	13
Performance Metrics for Expensive Programs	15
Surface Inspectors Offer Limited Security Benefit.....	15
Chapter 4: Support Private Sector Job Growth	17
Companies Deterred by TSA’s Unpredictability	17
Some Airports Keep Federal Screeners to Avoid Damaging Relationship with TSA.....	18
Chapter 5: Eliminate Unnecessary or Burdensome Regulations	19
Trucking Regulations Are Redundant	19
Sluggish Rulemaking Process.....	20
Prohibited Items List.....	21
Emergency Amendments.....	21
Appendix A: Select Correspondence from the 112th Congress	23

CHAPTER 1: REFOCUS ON SECURITY MISSION

THE GLOBAL TRANSPORTATION NETWORK

The United States is not alone in the war against terrorism. Al-Qaeda and its affiliates are tirelessly working to exploit any weaknesses within the global transportation network including targeting countries with lenient aviation security standards. Most of the recent terrorist activity against U.S. aviation has originated abroad in countries with less stringent standards, such as Yemen. In October 2010, two explosive devices originating from Yemen were found aboard cargo planes in Britain and Dubai bound for the United States. The explosive devices were hidden within printer cartridges and assembled by members of al-Qaeda in the Arabian Peninsula. The plot was disrupted based on an intelligence tip, but the close-call scenario proves TSA and other federal agencies have a lot of work to do, in cooperation with our foreign partners. We cannot rely solely on intelligence to stop the next attack. It is TSA's responsibility to represent U.S. interests and work toward harmonization of standards for both passenger and all-cargo aircraft and ensure those standards are continuously strengthened. To that end, TSA participates in meetings and deliberations of the International Civil Aviation Organization among other global activities. However, disparities in security standards still exist. The Subcommittee Staff believes TSA has failed to effectively implement its mandate because the agency maintains a reactive approach to security; does not adequately test new technologies and procedures; and ultimately is too bogged down in managing its bloated federal workforce.

The illustration below depicts TSA's reactive posture that has persisted since 9/11. Once a procedure is put in place, it is almost never removed.



SECURITY BREACHES OCCURRING AT AIRPORTS



Countless security requirements are imposed on U.S. travelers. But as external scrutiny reveals TSA often does not follow its own security obligations behind the scenes. In May 2012, the Department of Homeland Security Inspector General released a report entitled “Transportation Security Administration’s Efforts to Identify and Track Security Breaches at Our Nation’s

Airports.” The Inspector General reviewed six Category X airports from January 2010 through May 2011. According to the report, an internal TSA reporting system known as Performance and Results Information System (PARIS), which TSA staff are required to update if a security breach occurs, has been woefully underutilized.¹ Over a 15-month period of time, the Inspector General identified that only 42% of security breaches reviewed in files were reported in PARIS.² Of those security breaches that were properly reported, the Inspector General could only identify corrective action being taken by TSA in 53% of those incidents.³

While TSA has several programs that report and track security breaches such as the PARIS system, the Inspector General found that TSA does not have a comprehensive oversight program in place to gather information about all security breaches and therefore cannot use the information to monitor trends or make general improvements to security. Additionally, the report found that TSA does not provide the necessary oversight to ensure that all breaches are consistently reported, tracked, and corrected. As a result, the agency does not have a complete understanding of breaches occurring at the Nation’s airports and misses opportunities to strengthen aviation security.⁴ The Inspector General recommended that TSA refine its definition of what constitutes a security breach and develop a comprehensive plan to ensure that security breaches are accurately reported based on the new definition.

At a May 2012 Subcommittee hearing entitled “Access Control Point Breaches at Our Nation’s Airports: Anomalies or Systemic Failures?” TSA agreed with the Inspector General’s findings and insisted it would correct the problem.⁵ While it is encouraging that TSA is finally taking steps to improve the way it tracks and identifies security breaches based on the report, the Subcommittee

¹ U.S. Department of Homeland Security Office of Inspector General, *Transportation Security Administration’s Efforts to Identify and Track Security Breaches at Our Nation’s Airports*, OIG-12-80 (Washington, D.C.: May 2012).

² Ibid.

³ Ibid.

⁴ Ibid.

⁵ Access Control Point Breaches at Our Nation’s Airports: Anomalies or Systemic Failures?: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security, 112th Cong., 2nd Sess., May 15, 2012.

Staff questions whether TSA would have corrected the problem on its own if the Inspector General had not exposed it. Moreover, travelers lose confidence in TSA and the security requirements imposed on them when evidence shows significant weaknesses in TSA internal controls.

FLIGHT STUDENTS ARE NOT PROPERLY VETTED

The 9/11 hijackers exposed a gaping hole in the security of U.S. flight schools, which resulted in the federal government establishing the Alien Flight Student Program. For seven years, TSA has been responsible for vetting foreign flight students under this program. However, in July 2012, the Government Accountability Office (GAO) reported that significant weaknesses in flight school security persist.

TSA's inaction raises significant concern over its focus on fulfilling its security obligations and staying ahead of the next potential threat.

A July 2012 Subcommittee hearing revealed that not only was TSA unable to account for all foreign nationals taking flight training in the U.S. as reported by the GAO, but that U.S. citizens on the No Fly List could receive flight training, including flying unaccompanied.⁶

Congress gave TSA broad authority to conduct necessary security checks on flight school candidates in December 2003⁷, but incredibly, TSA allowed this No Fly List loophole and other weaknesses to persist. TSA's inaction raises significant concern over its focus on fulfilling its security obligations and staying ahead of the next potential threat.

It is worth noting that U.S. general aviation contributes more than \$150 billion to our economy every year and employs over one million people.⁸ The U.S. flight training industry is highly successful in preparing U.S. citizens and foreign nationals for private and commercial flight and relies on TSA to ensure students are properly vetted. This industry deserves to see marked improvement from the federal government in flight student vetting.

THE VALUE OF EXPLOSIVES DETECTION CANINE ASSETS

TSA's National Explosives Detection Canine Team Program trains canines and handlers to assist with the security screening of both passengers and air cargo and to support surface transportation security operations. The Subcommittee has consistently heard from industry, TSA leadership, and

⁶ A Decade After 9/11 Could American Flight Schools Still Unknowingly Be Training Terrorists?: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security, 112th Cong., 2nd Sess., July 18, 2012.

⁷ *Vision 100 – Century of Aviation Reauthorization Act*. Public Law 108-176, December 12, 2003, 117 Stat. 2490.

⁸ A Decade After 9/11 Could American Flight Schools Still Unknowingly Be Training Terrorists? Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 2nd Sess., July 18, 2012.

... substantial delays are leading to a missed opportunity to expand canine resources, create private sector jobs and leverage the private sector toward better air cargo security.

the Secretary of Homeland Security that canines are a critical tool for explosives detection. At a March 2011 Subcommittee hearing focused on air cargo security, TSA testified that explosives detection canine teams “are one of our most reliable resources for cargo screening.”⁹

And yet, substantial delays are leading to a missed opportunity to expand canine resources, create private sector jobs and leverage the private sector toward better air cargo security. TSA needs to finalize its efforts to develop a certification program for private companies to

enable them to use their own canines, certified to TSA standards, to meet federal air cargo screening mandates. Leveraging private sector resources will introduce much-needed additional canines into the cargo screening system.

In addition to cargo, the number of canine teams deployed to screen air passengers is on the rise, with many law enforcement and security professionals recognizing the broad applicability of this vital resource in the airport environment. Unfortunately, it would take many years at TSA’s current pace just to cover Category X airports with a minimum number of these teams, much less surface modes of transportation.

Finally, TSA should work with our foreign partners to develop international standards for explosives detection canines to ensure that passenger and all-cargo aircraft are screened to the same standard at foreign airports with flights bound for the U.S.



Recommendations:

- ***Prioritize the harmonization of aviation security standards worldwide***
- ***Adopt a comprehensive plan to mitigate evolving threats***
- ***Expand the use of canine explosives detection assets***

⁹ Securing Air Commerce From the Threat of Terrorism: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 1st Sess., March 9, 2011.

CHAPTER 2: PASSENGER EXPERIENCE & PRIVACY PROTECTIONS

In many ways, TSA has become its own worst enemy by underestimating the privacy impact of its operations, and limiting lines of communication and the flow of information to the public. The American people could be more supportive of TSA if they understood why TSA was implementing a particular policy or procedure and what threat or vulnerability it was addressing. Instead, in the last eleven years the American people have become increasingly more critical of TSA.

The implementation of enhanced pat-downs in October 2010 marked a critical turning point in the relationship between TSA and travelers. In its public statement of this new procedure TSA stated that, “pat-downs are one important tool to help TSA detect hidden and dangerous items such as explosives.”¹⁰ While TSA did make a brief statement on this significant change, its immediate rollout and shoddy implementation left travelers confused and frustrated.

Pat-downs have hit a nerve with the general public, and TSA has failed to adequately explain why it continues to use this procedure two years after its initial rollout.

Pat-downs were initiated in direct response to a serious, imminent, ongoing terrorist threat. That TSA continues to garner public resentment from this procedure is indicative of TSA missing the mark both on implementation (e.g. waiting a year to realize children should not be subject to full-body pat-downs by adults, particularly without parental consent) and communication. Pat-downs have hit a nerve with the general public, and TSA has failed to adequately explain why it continues to use this procedure two years after its initial rollout.

TSA must work to improve its relationship with the traveling public by respecting travelers’ privacy and treating them as partners in our mutual desire for secure transportation systems.

The Department of Homeland Security and state and local transportation systems, for example, utilize the ‘See Something, Say Something’ campaign across the country to engage travelers.¹¹ TSA could better utilize the visibility of the public and ask for help in reporting suspicious activity. By encouraging travelers to become an active additional security layer, TSA can remind travelers of the shared goal of security and redefine the relationship between TSA and travelers as partners, not adversaries.

In addition to its relationship with the traveling public, TSA must improve its relationship with the Congress. At a July 2012 Subcommittee hearing focused on the future of transportation security, Ozzie Nelson from the Center for Strategic and International Studies pointed out that, “It will be impossible for TSA to improve its image significantly if government officials continue to use the agency as a source of political rhetoric. TSA can grow into a respected efficient and effective

¹⁰ See TSA Statement on New Pat-down Procedures at http://www.tsa.gov/press/happenings/102810_patdown.shtm>

¹¹ See If You See Something, Say Something™ Campaign at <http://www.dhs.gov/if-you-see-something-say-something-campaign>>

institution only if it is depoliticized.”¹² The rhetoric in Congress is largely a reflection of the general public’s attitude towards TSA. TSA needs to conduct a comprehensive analysis of its communications efforts in order to better articulate its policies, and improve its overall relationship with the American people.

RISK-BASED SCREENING INITIATIVES

In 2011, TSA began to acknowledge the public’s insistence that the agency adopt a more common sense, intelligence driven security approach. TSA launched a series of risk-based initiatives aimed at improving passenger experience including Pre✓, an expedited screening process for highly frequent flyers and other known travelers. Unfortunately, TSA has failed to adequately inform most travelers, and has failed to properly implement these initiatives to maximize their effectiveness.

Under Pre✓, for example, highly frequent air travelers and U.S. citizens enrolled in any one of U.S. Customs and Border Protection’s (CBP) Trusted Traveler programs are eligible to receive expedited screening benefits at TSA security checkpoints. These benefits include no longer removing shoes, laptops, light jackets, and belts. While TSA touts the program as a success, Pre✓ remains highly selective and inaccessible to most travelers. In most cases, members of the military, security clearance holders, and even those who signed up and paid \$180 for “Clear,” a TSA-sponsored Pre✓ predecessor, are still not eligible. The functionality of this program is further limited because travelers who are eligible for TSA Pre✓ on one airline are not eligible for TSA Pre✓ if they travel on a different airline. Common sense dictates that one’s risk-level should not change based on which airline he or she is flying on a given day.

Still, there is a bigger problem than eligibility for this program. TSA does not have an overarching plan for making significant changes in personnel, technology, and security operations to move toward a truly risk-based screening process. Further, the private sector, which once had a seat at the table, has been all but shut out of Pre✓.

... the private sector, which once had a seat at the table, has been all but shut out of Pre✓.

The Subcommittee Staff believes the private sector could help develop solutions to TSA’s most complex challenges. With enough flexibility, it could help transform the screening process into one that balances security needs with the traveler’s right to privacy. TSA should rely on the ingenuity of the private sector to reform, modernize, and automate the passenger screening process to the extent possible.

¹² Challenging the Status Quo at TSA: Perspectives on the Future of Transportation Security: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 2nd Sess., July 10, 2012.

MISSED DEADLINE FOR REVISED MILITARY SCREENING PROCEDURES



Public Law 112-86, the “Risk-Based Security Screening for Members of the Armed Forces Act, was signed by the President on January 3, 2012. This legislation was introduced on May 10, 2011 by Subcommittee Member, Congressman Cravaack (R-MN) and passed the House unanimously with a roll call vote of 404-0.¹³

The Act requires TSA, in consultation with the Department of Defense, to develop and implement a plan to provide expedited security screening for any member of the U.S. military, and any accompanying family member, to the extent possible, when he or she is in uniform and traveling on official orders. The Act requires TSA to implement the plan within 180 days of enactment, making the implementation date July 2, 2012.

As of September 2012, TSA had neither submitted a plan to Congress nor implemented such a plan. Even though an expedited screening process exists under Pre✓ at 23 airports throughout the country, active duty service members are only eligible for Pre✓ at two of those airports - Ronald Reagan Washington National Airport and Seattle-Tacoma International Airport.

TSA needs to rapidly expand Pre✓ expedited screening benefits to active duty service members. In July 2012, the Subcommittee held a hearing to assess TSA’s delayed implementation of P.L. 112-86. At the hearing, TSA testified that it “expect[s] to move forward with full implementation to all Pre✓ cities by the end of calendar year 2013,” nearly a year and half after the deadline required by the law.¹⁴

WEAKNESSES IN BEHAVIOR DETECTION PROGRAM

In addition to screening operations at security checkpoints, TSA also observes passenger behavior inside the airport under the Screening of Passengers by Observation Techniques (SPOT) program. TSA personnel are trained to detect individuals exhibiting suspicious behaviors that indicate they may be a threat to transportation security. Individuals exhibiting specific behaviors may be referred for additional screening at the checkpoint. Those referrals are supposed to be based solely on behaviors, not on appearance, race, ethnicity or religion.

In April 2011, DHS’ Science and Technology Directorate reviewed the SPOT program and completed a Validation Study Report, which was reviewed by TSA. The study, however, was not designed to comprehensively validate whether SPOT could be used to reliably identify individuals in

¹³ See Final Vote Results for Roll Call 862 at <http://clerk.house.gov/evs/2011/roll862.xml>

¹⁴ Has TSA Met the Deadline to Provide Expedited Screening to Military Service Members?: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 2nd Sess., July 11, 2012.



an airport environment who pose a security risk. Rather, the study was designed to assess the effectiveness of the indicators used to determine high-risk travelers. The study found that SPOT's selection of high-risk travelers is nearly nine times higher than random selection at detecting any considered outcome (arrest, false or fraudulent documents, and serious prohibited/illegal items).¹⁵

In July 2011, GAO recommended that an independent panel of experts help to develop a comprehensive methodology to determine if the SPOT program is based on valid scientific principles that can be effectively applied in an airport environment for counterterrorism purposes.¹⁶ That recommendation has gone unresolved.

While TSA's SPOT program is theoretically modeled off of the interview screening techniques employed by the Israeli government at Ben Gurion International Airport, it remains difficult to fully utilize the Israeli model in the United States based on the sheer passenger volume differences that exist, among other key differences. Israel has just one major airport, with roughly 12 million passengers traveling through it in a given year. In contrast, the busiest airport in the United States, Atlanta Hartsfield-Jackson airport, sees over 43 million passengers in a year. In fact, the 19 busiest airports in the U.S. all see substantially more than 12 million passengers in a given year.

Given the cost of the program, recent allegations of racial profiling, and broad concerns as to its actual impact on security, TSA should look to further validate the SPOT program and assess if there is a value added to aviation security.

HEALTH AND PRIVACY CONCERNS ABOUT ADVANCED IMAGING TECHNOLOGY

There are currently 754 Advanced Imaging Technology (AIT) machines deployed across the United States.¹⁷ In February 2011, TSA Administrator John Pistole testified before the Subcommittee that "the radiation dose from backscatter AIT machines has been independently evaluated by the Food and Drug Administration, the National Institute of Standards and Technology, and the Johns Hopkins University Applied Physics Laboratory, all of which have affirmed that the systems comply with established standards for safety."¹⁸ However, in March 2011, TSA reported that there had been

¹⁵ Staff Briefing with TSA at TSA Headquarters, May 6, 2011.

¹⁶ U.S. Government Accountability Office, *Aviation Security: TSA Has Taken Actions to Improve Security, but Additional Efforts Remain*, GAO-11-807T, (Washington, D.C.: July 11, 2011).

¹⁷ Data provided by TSA Legislative Affairs Office via e-mail on August 3, 2012.

¹⁸ Terrorism and Transportation Security: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 1st Sess., February 10, 2012.

inaccurate contractor reporting concerning the test results for x-ray technologies deployed by TSA, including the backscatter AIT machines. While AIT's safety may have been evaluated in the past, TSA failed to validate subsequent safety testing by the contractor. This disclosure prompted Subcommittee Chairman Rogers to send Administrator Pistole a letter on March 11, 2011 demanding TSA institute better oversight.¹⁹

In addition to health concerns, the AIT machines have also raised privacy concerns. In July 2011, the U.S. Circuit Court of Appeals for the District of Columbia ruled that TSA needed to hold public hearings and adopt public rules about the use of AIT machines. A year later, TSA has failed to act on the court's ruling.²⁰

An AIT software upgrade known as Automated Target Recognition (ATR) enhances passenger privacy by eliminating person-specific images, and replacing them with generic human outlines. This software also provides a security enhancement with its ability to auto-detect items that could pose a potential threat.

While ATR is an important development for travelers' privacy, the software is only currently available on millimeter wave AIT machines, representing approximately two-thirds of all AIT machines deployed in the United States.²¹ To date, TSA has spent nearly \$8 million developing ATR, and will spend additional funds as it works to develop this software for the backscatter machines.

While AIT's safety may have been evaluated in the past, TSA failed to validate subsequent safety testing by the contractor.

Travelers deserve to see a concrete timeline for implementing ATR on all AIT machines, and a commitment from TSA to sponsor an independent analysis of the potential health impacts of the machines.

Recommendations:

- ***Enlist the private sector to modernize and, to the extent possible, automate the passenger screening process to reduce pat-downs***
- ***Implement privacy software on all AIT machines***
- ***Sponsor an independent analysis of the potential health impacts of AIT machines***

¹⁹ Appendix A: Letter to Administrator Pistole, March 11, 2011.

²⁰ Roberts, Christine. (2012, August 2). Federal appeals court slams TSA for ignoring hearings on scanner use. *New York Daily News*. Retrieved August 9, 2012, from, http://articles.nydailynews.com/2012-08-02/news/33005363_1_nonmetallic-items-body-scanners-tsa.

²¹ Data provided by TSA Legislative Affairs Office via e-mail on August 3, 2012.

CHAPTER 3: ELIMINATE WASTEFUL SPENDING

TSA'S BROKEN PROCUREMENT PROCESS

...TSA has still not addressed several fundamental flaws in its procurement process.

With an annual budget approaching \$8 billion and the tightening of budgets across the board, TSA must eliminate wasteful spending and find ways to do more with less.

In 2006, TSA spent \$29.6 million on 207 explosives trace portal (“puffer”) machines designed to blow air onto passengers and shake loose explosives particles that would then be detected.²² The puffer machines represented the first deployment of a checkpoint technology whose development had been initiated by TSA.²³ It turned out the machines had been inadequately tested and failed to work in dirty, humid airport environments. The machines were ultimately removed from service.

Despite the negative results of its first technology procurement six years ago, TSA has still not addressed several fundamental flaws in its procurement process.

“The system is going to cost over \$100 million...is it justifiable? I have not seen the cost-benefit analysis that clearly lays that out.”

For roughly three years, TSA worked to develop a Credential Authentication Technology/Boarding Pass Scanning System (CAT/BPSS). This technology is intended to verify the authenticity of passenger identifications (IDs) and boarding passes, and compare these two pieces of information to ensure a match. Following several site visits and briefings, in June 2012, the Subcommittee held a hearing that uncovered weaknesses in the technology, including a lack of cost-benefit analysis and integration with other security programs.²⁴

When asked if CAT/BPSS would identify a terrorist threat, Steve Lord of the Government Accountability Office (GAO) testified, “there have been some instances where in the past terrorists have been exposed and have used fraudulent IDs. But, again, you have to make the overall judgment. The system is going to cost over \$100 million...is it justifiable? I have not seen the cost-benefit analysis that clearly lays that out.”²⁵

After increased Congressional scrutiny and oversight, TSA postponed the purchase of CAT/BPSS.

²² Data provided by e-mail from TSA Legislative Affairs Office on September 5, 2012.

²³ U.S. Government Accountability Office, *DHS and TSA have researched, developed, and begun deploying passenger checkpoint screening technologies, but continue to face challenges*, GAO-10-128 (Washington, D.C.: October 2009).

²⁴ Is TSA's Planned Purchase of CAT/BPSS a Wise Use of Taxpayer Dollars?: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security, 112th Cong., 2nd Sess., June 19, 2012.

²⁵ Ibid.

In October 2009, GAO reported more broadly that TSA had not yet completed a cost-benefit analysis to prioritize and fund airport screening technology investments, in part because it had not yet developed life-cycle cost estimates for its various screening technologies.²⁶ GAO found that, given the cost of various technologies, a cost-benefit analysis would help decision makers determine which technology provides the greatest mitigation of risk for available resources.

In Fall 2011, the Subcommittee held a series of hearings about reforms in TSA technology development and procurement that could spur much-needed job growth in the private sector. Over the course of these hearings, several themes emerged as critical to TSA technology reform:

- **Transparency:** Early and open communication with the private sector is essential. TSA needs to foster greater openness with industry, so potential vendors know what to expect from TSA. Further, technology manufacturers have indicated that TSA should have early dialogue with industry regarding the technological realm of possibility in order to set attainable standards.
- **Program Management:** TSA has begun to realign its offices under a new organizational structure. It remains to be seen if this will allow for improved coordination and accountability for procurement decisions. Some companies have previously reported a significant disconnect inside TSA between its procurement officials and technology experts.
- **Testing and Evaluation:** Technology testing is a consistent industry concern. The process is often lengthy and frustrating. To improve the process, third party certification of technologies could be done, for example, through the outsourcing of certification to an independent laboratory on a fee-for-service basis.

Technology procurement missteps have a large quantifiable cost to taxpayers. TSA must take immediate steps to reflect on its technology procurement challenges and implement necessary reforms in order to eliminate the wasteful technology expenditures that do not make Americans safer.

TSA PERSONNEL COSTS

TSA's wasteful spending is not limited to technology; it has employed counterintuitive hiring practices during an economic downturn. To date, TSA employs roughly 62,000 people, including over 47,000 screeners, a number that has consistently grown over the last several years.

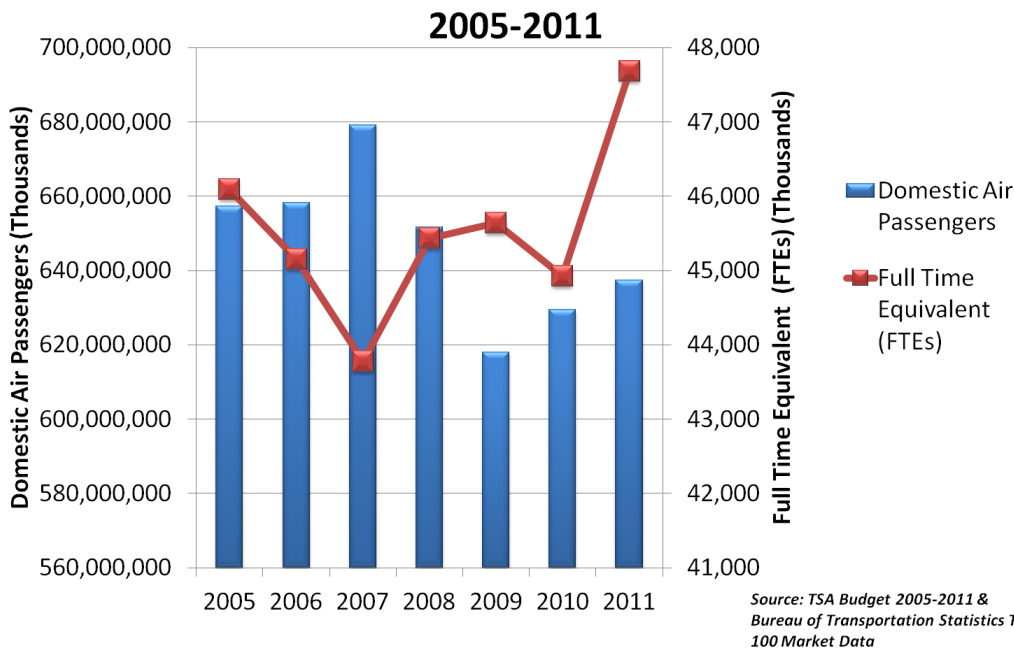
TSA should examine its growing number of employees given the net decrease in the number of people traveling each year in the U.S. Payroll, compensation, and benefits for the TSA screener workforce now total more than \$3 billion every year - half of TSA's budget.

²⁶ U.S. Government Accountability Office, *DHS and TSA have researched, developed, and begun deploying passenger checkpoint screening technologies, but continue to face challenges*, GAO-10-128 (Washington, D.C.: October 2009).

A private sector entity in the face of a shrinking customer base must downsize. TSA, by contrast, has continually grown its ranks despite fewer travelers, an economic downturn, and purchasing expensive new screening technology.

A private sector entity in the face of a shrinking customer base usually must downsize. TSA, by contrast, has continually grown its ranks despite fewer travelers, an economic downturn, and purchasing expensive new screening technology. There does not appear to be a correlation between TSA’s staffing model and the number of travelers that need to be screened. The following figure illustrates the increasing size of the screener workforce relative to the number of domestic air travelers.

Transportation Security Officer (TSO) Full Time Equivalent (FTEs) vs. Domestic Air Passengers:



Finally, in July 2012, the Subcommittee received testimony from Dr. Richard Bloom, Associate Vice President for Academics and the Director of Terrorism, Espionage and Security Studies at Embry-Riddle Aeronautical University. Dr. Bloom has extensive background in aviation security threat assessment, terrorism, and intelligence collection. When asked by Subcommittee Chairman Rogers, “...what’s the one thing you would change immediately about TSA?” Dr. Bloom replied, “I would

take maybe 20 to 30 percent of the [TSA] resources and put it into intelligence collection analysis and then use that to apprehend and detain and neutralize more adversaries of the U.S. government.”²⁷

PERFORMANCE METRICS FOR EXPENSIVE PROGRAMS

At an annual cost of \$89 million, TSA’s Visible Intermodal Prevention and Response (VIPR) teams work with local law enforcement officials at their request to supplement existing security resources, such as canine teams.²⁸ VIPR is intended to improve deterrence and detection capabilities, and introduce an element of unpredictability into transportation systems in order to disrupt potential terrorist planning activities. While these are important goals, criticism has been raised about the effectiveness of VIPR teams.

In June 2008, the DHS Office of Inspector General reported that although TSA made progress in addressing problems with early VIPR deployments, TSA still lacked coordination with local transit officials.²⁹ In a review of the President’s FY 2012 Budget Request, GAO reported that performance measures had not been fully established to assess the results of VIPR deployments. TSA agreed that performance measures needed to be developed for VIPR teams, and pledged to develop such metrics, including measuring interagency collaboration and stakeholder views on the effectiveness of VIPR teams.³⁰ However, TSA has since admitted that performance metrics are difficult to develop for this program.

The lack of performance metrics is not unique to VIPR teams. TSA’s \$222 million per-year Screening Passengers by Observation Technique (SPOT) program and the \$50 million per-year Surface Transportation Security Inspection program³¹ currently do not have established performance metrics either, calling into question the validity of those programs as well.

SURFACE INSPECTORS OFFER LIMITED SECURITY BENEFIT

In 2005, TSA created the Surface Transportation Security Inspection program to provide oversight and security assistance to the rail, mass transit, highway, and pipeline sectors. TSA’s surface inspectors have authority to enforce federal regulations and help stakeholders improve security. In two years, TSA more than doubled the size of the surface inspector workforce, from 175 inspectors in 2008 to 404 inspectors in 2010. By 2012, the Surface Transportation Security Inspection program had an annual budget of \$54.8 million dollars, 40% of TSA’s overall surface transportation budget.

²⁷ Challenging the Status Quo at TSA: Perspectives on the Future of Transportation Security: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 2nd Sess., July 10, 2012.

²⁸ Data provided by e-mail from TSA’s Office of Legislative Affairs on September 7, 2012.

²⁹ U.S. Department of Homeland Security Office of Inspector General, *TSA’s Administration and Coordination of Mass Transit Security Programs*, OIG-08-66 (Washington, D.C.: June 2008).

³⁰ U.S. Government Accountability Office, *Transportation Security: Additional Actions Could Strengthen the Security of Intermodal Transportation Facilities*, GAO-10-435R (Washington, D.C.: (May 2010).

³¹ Data provided by TSA Legislative Affairs Office via e-mail on September 7, 2012 and May 21, 2012 respectively.

Surface Inspector Budget Information ³²						
Year	FY 08	FY 09	FY 10	FY 11	FY 12	FY 13
Cost (Millions)	16.6	21.3	50.7	48.7	54.8	49.8
Full Time Equivalents (FTEs)	175	225	404	404	404	404

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) mandated that the DHS Inspector General conduct an assessment of the performance and effectiveness of the surface inspectors. The Inspector General’s 2009 report stated, “As TSA expands its presence in non-aviation modes, it must look critically at how it is deploying its resources.”³³

When asked during a July 2011 Subcommittee hearing about the impact of surface inspectors on security, Association of American Railroad’s Assistant Vice President and former TSA employee Tom Farmer stated, “...because the TSA surface inspectors are supervised locally, the priorities they pursue, the interpretations of the regulations that they bring to bear, can vary significantly from place to place.” Mr. Farmer went on to say that, “...the rapid increase of the workforce has caused a departure from what was the fundamental premise of the hiring of those inspectors at the outset of the program in 2005...There was very much then a focus on hiring people with a rail background...[now] they don’t have extensive rail or transit experience.”³⁴

At the same hearing, Chief of Police for Atlanta’s mass transit system Wanda Dunham testified, “One thing to keep in mind is that the increase in security inspectors does not mean more security. I think people get confused by that. They are kind of an oversight. And sometimes it is a little bit much for them to come in...yet another inspector to come in. I need more boots on the ground. I need more people in the field.”³⁵

At a May 2012 Subcommittee hearing on the surface inspectors program, these sentiments were echoed by stakeholders representing the trucking, bus, freight and passenger rail industries.³⁶ At the hearing, industry witnesses unanimously agreed the inspectors program was in need of reform. TSA needs to seriously consider the criticism of the Surface Transportation Security Inspection program by the transit systems the inspectors are designed to help protect.

³² Data provided by TSA Legislative Affairs Office via e-mail on May 21, 2012.

³³ U.S. Department of Homeland Security Office of Inspector General, *Effectiveness of TSA’s Surface Transportation Inspectors*, OIG-09-24 (Washington, D.C.: February 2009).

³⁴ Industry Perspectives: Authorizing the Transportation Security Administration for FY 2012 and 2013, Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 1st Sess., July 12, 2011.

³⁵ Ibid.

³⁶ TSA’s Surface Inspection Program: Strengthening Security or Squandering Scant Resources?: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security, 112th Cong., 2nd Sess., May 31, 2012.

Recommendations:

- ***Reduce the size of the TSA workforce***
- ***Conduct cost-benefit analyses for all major programs and purchases***
- ***Communicate with industry to avoid setting technology requirements that are unattainable***

CHAPTER 4: SUPPORT PRIVATE SECTOR JOB GROWTH

From the field to headquarters, TSA has held on strongly to its ‘government knows best’ mentality. In part, this approach is supported by those who try to argue that TSA was created to do the job the private sector failed to do on 9/11. However, there is a crucial fact missing from that argument, which is that the layered security measures and government oversight that exists today did not exist in the airport environment before 9/11 when contractors performed screening functions. More importantly, even though the government quickly federalized aviation security and the screening workforce after 9/11, it does not mean it is the best approach for us today.

COMPANIES DETERRED BY TSA’S UNPREDICTABILITY

Technology companies struggle with having to predict TSA’s future procurement plans. The Subcommittee Staff has heard from several industry stakeholders that a five-year spend plan from TSA would help them invest in new security technologies, knowing they may have a customer like TSA down the road. Without such a plan, companies are left to take TSA at its word, and oftentimes TSA switches direction without so much as a phone call to the prospective companies involved. One technology company expressed frustration at having worked to develop a liquid scanning technology based on TSA’s stated goals, only to be told by TSA afterward that it had changed course and was no longer interested in this type of technology.

Technology companies struggle with having to predict TSA’s future procurement plans.

Another company shared with the Subcommittee Staff that it had avoided working with TSA under the Screening Partnership Program because of a lack of transparency. TSA has been unwilling to share the breakdown of its own screening costs, so companies are left scratching their heads as to how to prove they can perform screening operations at a lower cost than TSA.

SOME AIRPORTS KEEP FEDERAL SCREENERs TO AVOID DAMAGING RELATIONSHIP WITH TSA

Under TSA's Screening Partnership Program (SPP), airports can apply to opt-out of using federal screeners in favor of private screeners. Some airports, however, may choose not to apply to SPP, even if they would rather use private screeners, for a variety of reasons. Instead, these airports have reluctantly chosen to keep the status quo with federal screeners.

In February 2012, the Subcommittee held a hearing entitled "Screening Partnership Program: Why is a Job-Creating, Public Private Partnership Meeting Resistance at TSA?"³⁷ At the hearing, Mark VanLoh, Director of Aviation for Kansas City, stated that more airports are moving in the direction of privatization. He said:

If TSA took steps to expand the private sector's role in the airport environment, new companies would step up to fill the need and TSA could assume a regulatory role, rather than an operational and regulatory role.

"I get that every week from fellow airport directors all around the country. There are about 400 of us in the United States that run airports of any size. Early on in the program, there was word out that if you privatized your screening and something happened, and somebody maybe got a weapon through and an aircraft went down, your airport would be sued out of existence. That scared a lot of cities away from this program. Well, that was false. That is not the case. Lately, a lot of airports were concerned about TSA's oversight going forward if they wanted to elect out. So there are, in fact, many airports that want to do this today."³⁸

TSA will not accept the use of private screeners except under limited terms and conditions. At a July 2012 Subcommittee hearing, Bob Poole of the Reason Foundation testified that TSA has a built-in conflict of interest because it self-regulates.³⁹ This conflict, Poole argues, could be mitigated with greater private sector involvement, especially at the checkpoint. If private companies performed screening operations at airports, TSA could renew its focus on intelligence-driven, risk-based security.

If TSA took steps to expand the private sector's role in the airport environment, new companies would step up to fill the need. TSA could assume a regulatory role, rather than an operational *and* regulatory role. This may require TSA to pre-certify a list of private screening companies to compete for contracts.

³⁷ Screening Partnership Program: Why is a Job-Creating, Public-Private Partnership Meeting Resistance at TSA?: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security, 112th Cong., 2nd Sess., February 16, 2012.

³⁸ Ibid.

³⁹ Challenging the Status Quo at TSA: Perspectives on the Future of Transportation Security: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security, 112th Cong., 2nd Sess., July 10, 2012.

Conducting vigorous oversight and providing companies with enough incentive and flexibility to perform will require fundamental changes at TSA.

Recommendations:

- ***Contract with the private sector to perform screening***
- ***Establish a five-year procurement plan to guide future investments in aviation security technology research and development***

CHAPTER 5: ELIMINATE UNNECESSARY OR BURDENSOME REGULATIONS

TRUCKING REGULATIONS ARE REDUNDANT

In February 2009, the U.S. Small Business Administration added eliminating “duplicative security background checks for commercial truck drivers” to its Top 10 Rules for Review and Reform.⁴⁰ To address this problem, Subcommittee Chairman Rogers introduced H.R. 1690, the MODERN Security



Credentials Act. This legislation would end the requirement for truck drivers to get both a Hazardous Materials Endorsement Security Assessment (to carry Hazardous Materials) and a Transportation Security Worker Identification Credential (TWIC) (to drive onto a port or other secure facility). In addition, the MODERN Security Credentials Act would reduce the population of drivers that need a security threat assessment. Currently, drivers carrying Hazardous Materials without a security or

terrorism nexus (such as paint or food coloring) must get a threat assessment. The legislation would direct the Secretary of Homeland Security to establish a list of ‘security-sensitive’ materials, and only drivers carrying those materials would be required to get a TWIC.

The regulatory redundancy imposed on truckers has carried on for long enough. There have been several good faith efforts to address the problem, but ultimately it will take legislative action to resolve.

⁴⁰ “Two New Regulations Added to 2009 R3 Top 10 Rules For Review And Reform,” *US Small Business Administration Office of Advocacy*, Press Release # 09-07 ADVO, 27 Feb 2009, from: <http://www.sba.gov/advocacy/809/12400>.

SLUGGISH RULEMAKING PROCESS

Over the years, TSA has become infamous for publishing notices of proposed rulemaking but later failing to issue final rules in an expeditious manner.

For example, in 2003 Congress directed DHS to develop a program to ensure security of domestic and international aircraft repair stations.⁴¹ After no action was taken, in 2007 Congress mandated that TSA issue a final rule on aircraft repair station security by August 2008, otherwise the Federal Aviation Administration (FAA) would no longer be authorized to certificate new foreign repair stations for U.S.-bound aircraft. TSA missed the deadline, and FAA certifications of new foreign repair stations came to a halt.

This delay has had significant economic consequences for American general aviation manufacturers...

In November 2009, TSA published a Notice of Proposed Rulemaking (NPRM) for repair station security, with a comment period ending on February 19, 2010.⁴² Although the comment period ended over two years ago, TSA has yet to issue a final rule. This delay has had significant economic consequences for American general aviation manufacturers (see Appendix A), and potentially the security of air travelers.

Another long overdue security program is the Large Aircraft Security Program (LASP). In October 2008, TSA issued an NPRM that would require all U.S. operators of aircraft exceeding 12,500 pounds maximum take off weight to implement security programs that would be subject to compliance audits by TSA. The proposed regulation would have also required operators to verify that passengers were not on the No Fly and/or Selectee portions of the federal government's consolidated terrorist watch list.⁴³

In response to the October 2008 NPRM, TSA received over 7,000 comments highlighting concerns with its expansive new proposal. After weighing those comments and conducting meetings with stakeholders, TSA decided to revise the NPRM and is considering changes to the type of aircraft subject to TSA regulation; compliance oversight; watch list matching of passengers; prohibited items; scope of the background check requirements and the procedures used to implement the requirement; and other issues. Additionally, in the Supplemental NPRM, TSA plans to propose security measures for foreign aircraft operators. U.S. and foreign operators would implement

⁴¹ *Vision 100 – Century of Aviation Reauthorization Act*. Public Law 108-176, December 12, 2003, 117 Stat. 2490.

⁴² TSA Member Briefing on Aircraft Repair Station Security Rulemaking Status, March 22, 2012.

⁴³ See TSA Proposes Large Aircraft Security Program at <http://www.tsa.gov/press/releases/2008/1009.shtm>

commensurate measures under the new proposed rule. TSA's supplemental NPRM is expected to be issued in September 2012, roughly four years after the original NPRM was issued.⁴⁴

TSA's rulemaking process is in need of reform. TSA should issue a final rule with input from industry for both Foreign Aircraft Repair Station Security and the Large Aircraft Security Program by the end of this calendar year, and take immediate steps to ensure these types of delays are avoided in the future.

PROHIBITED ITEMS LIST

In April 2012, former TSA Administrator Kip Hawley argued that TSA should eliminate the prohibited items list (with the exception of banning obvious weapons) and allow liquids of any size to pass through the screening checkpoint.⁴⁵ Mr. Hawley asserts that the prohibited items list creates vulnerability within the system because screeners are trained to only look for specific types of items. Since civil aviation continues to be a highly attractive target for terrorists worldwide, Mr. Hawley believes that the prohibited items list is simply a list to inform terrorists of what items *not* to use during their next attack.⁴⁶

At a June 2012 Subcommittee hearing entitled "TSA's Efforts to Fix Its Poor Customer Service Reputation and Become a Leaner, Smarter Agency" the TSA Administrator testified that he had "looked at the prohibited item list and I think there are some opportunities for us there."⁴⁷ The Subcommittee Staff considers modifications to the prohibited items list to be an important first step in rebuilding the relationship between travelers and screeners at the checkpoint.

The prohibited items list should better reflect current and emerging threats and not distract screeners from truly suspicious and dangerous items.

EMERGENCY AMENDMENTS

The Aviation and Transportation Security Act of 2001 (P.L. 107-71) (ATSA) authorized the Administrator of TSA to issue security regulations and directives to protect transportation security on an emergency basis and without following the established regulatory process. ATSA does not limit the length of such regulations or directives, nor does it require TSA to share with industry stakeholders the threat origin or how it relates to them. TSA also does not distinguish between

⁴⁴ See General Aviation Security and Other Aircraft Operator Security at <https://www.federalregister.gov/regulations/1652-AA53/general-aviation-security-and-other-aircraft-operator-security->>

⁴⁵ Hawley, Kip. (2012 April 15). Why Airport Security is Broken – And How to Fix It. *The Wall Street Journal*. Retrieved July 25, 2012, from

<http://professional.wsj.com/article/SB10001424052702303815404577335783535660546.html?mg=reno64-wsj>>

⁴⁶ Ibid.

⁴⁷ Challenging the Status Quo at TSA: Perspectives on the Future of Transportation Security: Hearing before the Committee on Homeland Security, Subcommittee on Transportation Security. 112th Cong., 2nd Sess., July 10 2012.

emergency regulations that will be implemented for a limited period of time and those that may require permanent or long term implementation. This creates frustration among industry stakeholders bearing the financial burden of these regulations. TSA should work with industry to improve the regulatory process.

Recommendations:

- ***Work with stakeholders to streamline existing security regulations***
- ***Issue final rules for long overdue security programs***
- ***Reform the Prohibited Items List to better reflect evolving threats***

CONCLUSION

TSA's responsibility is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. In order to fulfill that responsibility, TSA must shift its policies and procedures to better reflect the terrorist threat. Eleven years after 9/11, the American people expect to see tangible progress in transportation security, with effective operations that respect both their privacy and their wallets. The private sector is best suited to this challenge, not the federal government. TSA should begin an immediate shift toward partnering with the private sector for passenger screening and other security operations.

APPENDIX A: SELECT CORRESPONDENCE FROM THE 112TH CONGRESS

On July 27, 2012, Subcommittee Chairman Rogers sent a letter to Secretary Napolitano on the U.S. Government Accountability Office report entitled, General Aviation Security: Weaknesses Exist in TSA's Process for Ensuring Foreign Flight Students Do Not Pose a Security Threat (GAO-12-875)

On July 19, 2012, Subcommittee Chairman Rogers, Rep. Walberg, Rep. Cravaack, Rep. Walsh, and Rep. Turner sent a letter to Administrator Pistole with follow-up questions to the Subcommittee hearing entitled, "A Decade After 9/11 Could American Flight Schools Still Unknowingly Be Training Terrorists?"

On July 13, 2012, Subcommittee Chairman Rogers sent a letter to Administrator Pistole on recommendations that were offered at the Subcommittee hearing entitled, "Challenging the Status Quo at TSA: Perspectives on the Future of Transportation Security." On August 28, 2012, the Subcommittee received a response letter from Administrator Pistole.

On July 11, 2012, Subcommittee Chairman Rogers sent a letter to Administrator Pistole on his concerns regarding TSA's plans to purchase and deploy Credential Authentication Technology/Boarding Pass Scanning Systems (CAT/BPSS).

On March 26, 2012, T.J. Schulz, Director of the Security Manufacturers Coalition, sent a letter to Subcommittee Chairman Rogers with recommended changes to TSA's procurement process.

On May 16, 2012, Subcommittee Chairman Rogers and Ranking Member Jackson Lee sent a letter to Administrator Pistole on the Department of Homeland Security Inspector General Report entitled, "Transportation Security Administration's Efforts to Identify and Track Security Breaches at Our Nation's Airports."

On March 27, 2012, Subcommittee Chairman Rogers and Rep. Walberg sent a letter to Secretary Napolitano on the Department of Homeland Security delayed rulemaking on Aircraft Repair Station Security.

On November 30, 2011, Subcommittee Chairman Rogers and Rep. Farenthold sent a letter to Administrator Pistole on TSA's storage facilities.

On October 14, 2011, Subcommittee Chairman Rogers sent a letter to Administrator Pistole on the September 27, 2011 ruling of the United States Court of Federal Claims in the case of FirstLine Transportation Security, Inc., vs. The United States and Akal Security, Inc.

On March 11, 2011, Subcommittee Chairman Rogers sent a letter to Administrator Pistole on inaccurate contractor reporting on AIT safety test results and TSA's failed oversight.

On February 17, 2011, Subcommittee Chairman Rogers sent a letter to TSA Assistant Administrator Sammon requesting information on security initiatives led by the Office of Transportation Sector Network Management.



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

July 27, 2012

The Honorable Janet Napolitano
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Dear Secretary Napolitano:

I am writing to follow up on a discussion we had at the Committee on Homeland Security hearing entitled, "Understanding the Homeland Threat Landscape" on July 25, 2012.

At the hearing you said that the GAO report entitled, General Aviation Security: Weaknesses Exist in TSA's Process For Ensuring Foreign Flight Students Do Not Pose a Security Threat (GAO-12-875) focused on problems with foreign nationals taking flight training while in the country illegally during 2010 and before. You also said that the report indicated that TSA and ICE had already fixed the problems with respect to the whole flight school system but had not yet formalized that fix in writing. As promised at the hearing, I have attached several excerpts from the report that proves otherwise.

Thank you for your prompt and personal attention to this issue. I look forward to continue working with you to ensure the security of our Nation's flight schools.

Sincerely,

A handwritten signature in black ink, appearing to read "Mike Rogers", written in a cursive style.

Mike Rogers
Chairman
Subcommittee on Transportation Security

July 2012

GENERAL AVIATION SECURITY

Weaknesses Exist in
TSA's Process for
Ensuring Foreign
Flight Students Do
Not Pose a Security
Threat



G A O

Accountability * Integrity * Reliability

TSA officials responsible for overseeing security threat assessments stated that the process for conducting criminal history record checks for AFSP is substantively the same as that used for other TSA screening and credentialing programs. While there is no information indicating that any foreign nationals seeking flight training should not have been allowed to do so because of unidentified criminal offenses, we believe that TSA should continue to work with the FBI on joint risk assessments of TSA's access to criminal history records for credentialing programs, including AFSP.

Immigration Violations

There have been instances of overstays or other immigration-related violations for foreign nationals taking flight training in the United States, most notably for three of the September 11 hijackers.⁴⁶ Specifically, three of the six pilots and apparent leaders were out of status on or before September 11, including two in overstay status.⁴⁷ AFSP was implemented to help address such security concerns. As previously discussed, as part of AFSP, TSA conducts security threat assessments for foreign nationals requesting flight training in the United States. According to TSA officials, the purpose of the security threat assessment, which includes a check of the Terrorist Screening Database and a criminal history records check, is to determine whether the foreign national requesting flight training presents a security threat; the checks are not designed to determine whether an applicant is in the country legally. As part of the security threat assessment, TSA also conducts reviews of DHS's TECS database to determine if any negative immigration-related information is associated with the foreign national seeking flight training. However, TSA officials acknowledged that it is possible for a foreign national to be approved by TSA through AFSP and to complete flight training after entering the country illegally or overstaying his or her allotted time to be in the country legally.

⁴⁶In-country overstays refer to nonimmigrants who have exceeded their authorized periods of admission and remain in the United States without lawful status, while out-of-country overstays refer to individuals who have departed the United States but who, on the basis of arrival and departure information, stayed beyond their authorized periods of admission.

⁴⁷See GAO, *Homeland Security: Overstay Tracking Is a Key Component of a Layered Defense*, GAO-04-170T (Washington, D.C.: Oct. 16, 2003).

In 2010, ICE investigated a Boston-area flight school after local police stopped the flight school owner for a traffic violation and discovered that he was in the country illegally. Twenty-five of the foreign nationals at this flight school had applied to AFSP and had been approved by TSA to begin flight training after their security threat assessment was completed; however, the ICE investigation and our subsequent inquiries revealed the following issues:

- Eight of the 25 foreign nationals who received approval by TSA to begin flight training were in “entry without inspection” status, meaning they had entered the country illegally.
 - Six of these foreign nationals were later arrested by ICE as a result of the investigation. TSA indicated 1 individual had been approved to begin flight training at two other schools, although the flight schools indicated that he did not complete training.
 - Three of the 8 foreign nationals in “entry without inspection” status obtained FAA airman certificates: 2 held FAA private pilot certificates and one held an FAA commercial pilot certificate.
- Seventeen of the 25 foreign nationals who received approval by TSA to begin flight training were in “overstay” status, meaning they had overstayed their authorized period of admission into the United States.
 - Sixteen of these were arrested by ICE as a result of the investigation.
 - Four of the 17 foreign nationals in “overstay” status obtained FAA airman certificates: 3 held FAA private pilot certificates and 1 held a commercial pilot certificate.
- In addition, the flight school owner held two FAA airman certificates. Specifically, he was a certified Airline Transport Pilot (cargo pilot) and a Certified Flight Instructor. However, he had never received a TSA security threat assessment or been approved by TSA to obtain flight training. He had registered with TSA as a flight training provider under AFSP.
- Further, TSA data indicated that an additional foreign national arrested as a result of this flight school investigation for “entry without inspection” had previously completed flight training through an airline.

According to the AFSP program manager, TSA reviews TECS to determine if the student has prior immigration violations, including

overstays.⁴⁸ However, the program manager stated that this TECS review is not designed to determine how long the student is authorized to stay in the country or whether the student had entered the country legally. Rather, if the TECS review indicates that the foreign national has previous immigration-related violations, such as overstaying the authorized period of admission, TSA is to conduct additional TECS queries to determine if the individual is eligible to receive flight training. Further, according to TSA, prospective flight students may apply for AFSP before entering the United States, rendering moot the question of whether the foreign national had entered the country legally or overstayed.⁴⁹

The AFSP program manager stated that even though the foreign nationals were later found to be overstays, at the time of the review and adjudication of their security threat assessments, they were determined to be in legal status. According to TSA, none of the individuals that TSA processed and approved under AFSP had derogatory information within TECS, and visa overstay information is contained within TECS. However, ICE data we reviewed indicated that 16 of the 17 foreign nationals associated with the flight school who were found by ICE to be in overstay status at the time of the investigation had already been in overstay status at the time they received AFSP approval to begin flight training. This includes the 4 foreign nationals who were able to obtain FAA airman certificates. Further, the AFSP program manager stated that foreign nationals who may have entered the country illegally but who did not have prior immigration violations, did not have a criminal history, or were not on the terrorist watch list, could be successfully vetted through an AFSP security threat assessment and approved to receive flight training. The program manager added that under the current AFSP process, TSA cannot always determine at the time of application if an individual entered the United States "without inspection" (illegally) because applicants can apply to AFSP more than 180 days prior to the start date of training and applicants are not necessarily in the United States at the time of application.

⁴⁸As previously discussed, in addition to the TECS review, the security threat assessment consists of a check of the prospective flight student's biographical information against the Terrorist Screening Database and a Criminal History Records Check.

⁴⁹Foreign nationals applying to AFSP have 180 days from the time they are approved to begin flight training in the United States to begin flight training. According to TSA, they may submit their applications before entering the country.

Senior officials from TSA and ICE stated that the agencies have initiated a process in which TSA and ICE check the names of AFSP applicants against the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program's Arrival and Departure Information System (ADIS) to help address this gap, as well as to identify foreign nationals taking flight training who become overstays.⁵⁰ Specifically, in March 2011, TSA vetted a list of current alien flight students in TSA's AFSP database against names in USVISIT's ADIS to determine if any were potential overstays. This review resulted in the identification of 142 possible overstays. In May 2011, TSA provided ICE with the results of its analysis, and ICE vetting further reduced the list of possible overstays to 22. In September and October of 2011, ICE initiated 22 investigations based on the results of this analysis, which resulted in three arrests.

According to TSA and ICE officials, this initial matching of names in the AFSP database against ADIS was conducted once to give the agencies an indication of how many foreign nationals seeking flight training in the United States may be in violation of their immigration status and what the workload associated with conducting such matches would be. Information from this review could then be used to initiate investigations of individuals suspected of being in the country illegally either by overstaying their allotted time in the country or who may have entered the country illegally. The TSA and ICE officials added, however, that such a process would have to be conducted more regularly to systematically identify foreign nationals taking flight training who may be in violation of their immigration status or who may have entered the country illegally. They stated that establishing a more regular process of matching names of foreign nationals in the AFSP database against ADIS would allow the agencies to better identify foreign nationals seeking flight training who have violated the terms of their admission as well as those who have entered the country illegally.

However, several issues related to how a name matching program would work are being considered, such as which agency would vet names in the

⁵⁰The US-VISIT program is an automated visitor system to integrate information on the entry and exit from the United States of foreign nationals. The purpose of US-VISIT is to enhance the security of U.S. citizens and visitors, facilitate legitimate trade and travel, and ensure the integrity of the U.S. immigration system. ADIS is a database that stores traveler arrival, status management, and departure data. Arrival and departure data are received from, among other things, air and sea carrier manifests and U.S. Customs and Border Protection data entries at ports of entry.

AFSP database against ADIS, and how frequently names associated with potential violations would be provided to ICE. ICE and TSA officials stated that they have not specified desired outcomes or time frames, or established performance measures to evaluate the success of the program. Standards for program management state that specific desired outcomes or results should be conceptualized, defined, and documented in the planning process as part of a road map, along with the appropriate steps and time frames needed to achieve those results.⁵¹ The standards also call for assigning responsibility and accountability for ensuring the results of program activities are carried out. Having a road map, with appropriate steps and time frames, and individuals assigned with responsibility and accountability for fully instituting a pilot program, as well as instituting that pilot program if it was found to help identify foreign nationals taking flight training who may be in violation of their immigration status or who may have entered the country illegally, could help TSA and ICE account for flight students with potential immigration violations, and thus better position TSA to identify and prevent a potential risk.

Conclusions

Since our 2004 report on general aviation security, TSA has taken steps to enhance communications and interactions with general aviation industry stakeholders as well as improve the vetting of foreign nationals enrolling in U.S. flight schools. AFSP was implemented to help prevent future occurrences of foreign nationals obtaining flight training to commit terrorist attacks, as they did for the September 11, 2001, attacks. Key to the effectiveness of this effort is the ability of TSA to conduct meaningful security threat assessments on foreign nationals seeking flight training to help determine whether these individuals pose a security threat. However, as shown in TSA's analysis, there are discrepancies between the data found in FAA's airmen registry and TSA's AFSP database, raising questions about whether some foreign nationals with airman certificates (pilot's licenses) have completed required security threat assessments. In addition, working with ICE to develop a plan that assigns responsibilities and accountability and time frames for assessing the joint TSA and ICE pilot program to identify foreign nationals who may have immigration violations—including those who entered the country illegally to obtain flight training—and instituting that program if it is found to be effective, could better position TSA and ICE to determine the benefits of

⁵¹Project Management Institute, *The Standard for Program Management* © (2006).



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

July 19, 2012

Honorable John S. Pistole
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Administrator Pistole:

On July 18, 2012, the Transportation Security Subcommittee held a hearing to discuss a Government Accountability Office (GAO) report regarding the Alien Flight Student Program (AFSP). During the course of the hearing, we were shocked to learn that individuals currently on the No Fly list are still able to receive flight training in the United States.

During questioning of the witnesses, there was not a consensus regarding TSA's current legal authority to vet those applying for flight schools against the No Fly list. Please respond immediately with the following information:

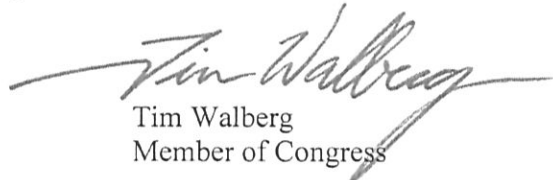
- Why is TSA not currently checking all prospective flight students against the No Fly list?
- Does current law allow TSA to establish a system to check U.S. citizens applying to flight schools against the No Fly list?
- If so, does TSA have the capability to establish a system that performs those checks?
- According to the GAO report, AFSP applicants undergo a Terrorist Screening Database check, which includes the No Fly list. If a foreign national is on the list, TSA analysts perform additional research to determine whether he or she is eligible to receive flight training. In what instances would a foreign national on the No Fly list be eligible to receive flight training?

Thank you for your prompt and personal attention to this matter. We are ready to work with you to ensure that this vulnerability is promptly addressed.



Mike Rogers
Chairman
Subcommittee on Transportation Security

Sincerely,



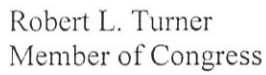
Tim Walberg
Member of Congress



Chip Cravaack
Member of Congress



Joe Walsh
Member of Congress



Robert L. Turner
Member of Congress



**One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515**

July 13, 2012

Honorable John S. Pistole
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Administrator Pistole:

On July 10, 2012, the Transportation Security Subcommittee held a hearing to discuss different perspectives on the future of transportation security. During the course of the hearing several recommendations were offered by the witnesses on ways to improve TSA's efficiency and effectiveness. I would like to share some of those ideas with you, and solicit your feedback as to the feasibility and/or timeline of taking action on them.

- 1) Establish a five to ten year term for the TSA Administrator that would transcend changes in Administration.
- 2) Empower TSA's 3,000+ checkpoint supervisors to intervene with more discretion in order to diffuse screening situations with unique or extenuating circumstances;
- 3) Increase the use of independent third party testing of security technologies;
- 4) Expand the Pre-Check program to include a greater number of trusted travelers from a variety of sources, including individuals with security clearances;
- 5) Recognize Pre-Check participants from one airline across all other Pre-Check participating airlines;
- 6) Better Leverage initiatives such as DHS' "If You See Something, Say Something" campaign, which capitalizes on the vigilance of travelers themselves; and
- 7) Pre-certify Screening Partnership Program contractors and empower airports to select a specific contractor from a pool of pre-certified options.

It is my continued hope that we can work together to keep the traveling public safe, while at the same time ensuring that TSA is operating in the most efficient and effective way possible. To that end, I believe these recommendations presented at the Subcommittee's recent hearing warrant your review and consideration. Within the next 30 days, please provide me with information on the feasibility of adopting each of the above outlined recommendations, and also address any legislative changes that would be required for implementation.

Thank you for your prompt and personal attention to this matter. I appreciate your efforts to secure the nation's transportation systems and look forward to working with you to improve TSA's performance in carrying out its critical mission.

Sincerely,

A handwritten signature in black ink, appearing to read "Mike Rogers". The signature is fluid and cursive, with the first name "Mike" and the last name "Rogers" clearly distinguishable.

Mike Rogers
Chairman
Subcommittee on Transportation Security



Transportation
Security
Administration

AUG 28 2012

The Honorable Mike Rogers
Chairman
Subcommittee on Transportation Security
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Rogers:

Thank you for your letter of July 13, 2012, soliciting feedback as to the feasibility of recommendations offered by witnesses during the July 10, 2012, hearing on the future of transportation security. This response provides the requested feedback for the seven recommendations.

1. Establish a five to ten year term for the TSA Administrator that would transcend changes in Administration.

In creating the Transportation Security Administration (TSA), the Aviation and Transportation Security Act established a term of five years for the position of Under Secretary of Transportation for Security within the U.S. Department of Transportation. In creating the U.S. Department of Homeland Security (DHS), the Homeland Security Act of 2002 (HSA) transferred TSA to DHS, but did not establish the position of the head of TSA as a statutorily mandated position appointed by the President, by and with the advice and consent of the Senate. The HSA did create specific Under Secretary positions as well as up to 12 Assistant Secretaries. The Secretary of DHS designated an available Assistant Secretary position as the head of TSA. Establishing a five to ten year term for the TSA Administrator would require new legislation.

2. Empower TSA's 3,000+ checkpoint supervisors to intervene with more discretion in order to diffuse screening situations with unique or extenuating circumstances;

I agree that providing discretion to properly trained, accountable, and responsible supervisory TSA field personnel to handle certain situations at a TSA checkpoint is appropriate. Last month, I approved a procedural change that allows Federal Security Directors to delegate greater discretion and decision-making authority to TSA managers and checkpoint supervisors to resolve alarms involving children 12 and under without requiring patdowns or other screening procedures. We are reviewing other circumstances in which this discretion could be expanded, such as with passengers 75 and older and service members in uniform.

3. Increase the use of independent third party testing of security technologies;

TSA supports independent third party testing, which can be achieved in several ways, depending on the type of testing. If the acquisition strategy requires system development, the Program Manager encourages the vendor to use and submit third party test results to supplement and replace as appropriate Government developmental testing. During the procurement phase, Government can encourage vendors' use of third party testing in support of their submitted data packages indicating that an accredited test provider has confirmed that their systems meet designated portions of TSA requirements. These test results can be used to significantly reduce the scope of testing accomplished and overseen by the Government. Equipment configuration must be strictly tracked. Additionally, TSA has competitively awarded test support contracts. Tests supported by these companies are overseen by a cadre of experienced test and evaluation experts. TSA also seeks specialized resources in the event additional expertise is required, such as the Johns Hopkins Applied Physics Laboratory. Test resources, such as those provided by third party test providers, can be used to augment TSA resources if the Government deems them qualified to do so. Only a government-designated Operational Test Agent may conduct the operational test and evaluation of candidate security products.

4. Expand the Pre-Check program to include a greater number of trusted travelers from a variety of sources, including individuals with security clearances;

TSA shares a common goal with you in looking for opportunities to further expand the pool of trusted travelers eligible for expedited screening. As an example, TSA agrees that individuals with certain security clearances are an important trusted population. We have been partnering closely, and carefully, with the Office of the Director of National Intelligence (ODNI) to allow us to include this population in a manner that protects the identity of those clearance holders. A Memorandum of Agreement (MOA) between TSA and ODNI was executed on March 8, 2012, to accomplish just what you proposed. The ODNI population was added to the Secure Flight system on May 8, 2012. Furthermore, our partnership with the Administrative Office of the U.S. Courts (AOUSC) has focused on enabling Federal judges, another trusted population, to access expedited screening. An MOA between TSA and AOUSC was executed on June 25, 2012. Federal judges were added to the Secure Flight system on June 27, 2012. We are also testing TSA Pre✓™ for members of the military at two locations, Ronald Reagan Washington National Airport (DCA) and Seattle-Tacoma International Airport (SEA). As TSA testified to your Subcommittee on July 11, 2012, TSA is closely partnering with the U.S. Department of Defense to create a list-based system of active military service members that will then qualify for TSA Pre✓™ at all participating airports. TSA will further continue our efforts to identify and incorporate trusted populations in an effort to capture the full security benefits of expedited screening and is actively doing so.

5. Recognize Pre-Check participants from one airline across all other Pre-Check participating airlines;

As of Spring 2012, TSA informed the airline industry that TSA would be amenable to an industry-provided solution that enables TSA Pre✓™ passengers from one airline to attain eligibility on another airline. Data exchange between airline providers would be the foundation of such a model. As of Summer 2012, airline association conversations are underway to explore this possibility.

While TSA is working with industry on these next steps I would like to emphasize that members of a U.S. Customs and Border Protection (CBP) Trusted Traveler program are able to access TSA Pre✓™ through any participating airline. To enroll in a CBP Trusted Traveler program, and to renew every 5 years, travelers must provide extensive biographic and biometric information to CBP and US-VISIT, as well as submit to terrorism, criminal, immigration, agriculture, customs violation, and other checks. Applicants must also complete a CBP officer interview of travel history. One of the incentives for a traveler to pursue CBP Trusted Traveler status is the ability to fly on any participating airline while on domestic travel through a participating airport.

6. Better Leverage initiatives such as DHS' "If You See Something, Say Something" campaign, which capitalizes on the vigilance of travelers themselves;

TSA and DHS strongly believe that homeland security is a shared responsibility of the American people, government at every level (Federal, state, local, tribal, and territorial), as well as the private sector and non-governmental organizations. The "If You See Something, Say Something™" campaign was launched in conjunction with the rollout of the Nationwide Suspicious Activity Reporting Initiative (NSI). The NSI is an administration-wide effort to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities. Led by the U.S. Department of Justice, the NSI is implemented in partnership with State and local officials across the Nation.

DHS, TSA, and other DHS components are strong participants in implementing the "If You See Something, Say Something™" campaign in cities and States, as well as transportation, private sector, universities, and law enforcement entities. DHS also provides significant support to fusion centers run by State and local officials. TSA partners with transportation stakeholders such as the American Public Transportation Association, the Aircraft Owners and Pilots Association, and the American Trucking Associations, to name a few, to leverage their members and transportation users in providing an additional layer of transportation security in all modes.

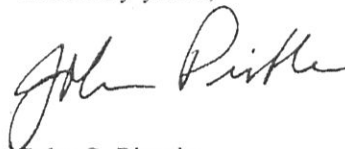
Both the "If You See Something, Say Something™" campaign and the NSI underscore the concept that homeland security begins with hometown security, where an alert public plays a critical role in keeping our nation safe.

7. Pre-certify Screening Partnership Program contractors and empower airports to select a specific contractor from a pool of pre-certified options.

To establish and maintain a pool of pre-certified Screening Partnership Program (SPP) contractors, application of the standards set forth in 49 USC § 44920 (c) (d) (e) would need to be demonstrated prior to obtaining certification. The initial investment cost associated with such a certification process is likely to be extensive and unrecoverable for potential contractors. In addition, 49 USC § 44920 requires the TSA Administrator to enter into the contract with the SPP service providers. Accordingly, our procedures for how we establish that relationship are governed by the Federal Acquisition Regulation (FAR). The FAR requires that Federal contracts using appropriated funds are awarded and administered by a Federal agency. Further, 49 USC § 44920 requires TSA to provide supervision and oversight to SPP service providers and authorizes TSA to terminate any contract entered into under SPP if the company has failed to meet specified requirements.

I appreciate that you took the time to share these ideas and hope this information is helpful. If you need additional information, please do not hesitate to contact me personally or the Office of Legislative Affairs at (571) 227-2717.

Sincerely yours,

A handwritten signature in black ink, appearing to read "John Pistle". The signature is written in a cursive, flowing style.

John S. Pistle
Administrator



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515
June 11, 2012

Honorable John S. Pistole
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Administrator Pistole:

I am writing to express my concerns regarding the TSA's plans to purchase and deploy Credential Authentication Technology/Boarding Pass Scanning Systems (CAT/BPSS). While CAT/BPSS may assist Transportation Security Officers in detecting fraudulent or invalid IDs and boarding passes, there are a number of weaknesses with this technology that call into question the benefit of deploying up to 1,400 units. On May 30, 2012, I appreciated the opportunity for my staff and I to receive a briefing and demonstration of CAT/BPSS at the TSA's Systems Integration Facility (TSIF). However, our discussion with the CAT/BPSS program team further reinforced our concerns, as outlined below.

As you know, the Subcommittee on Transportation Security has held a number of hearings on technology procurement reform at TSA. While we are beginning to see some improvements, including greater transparency with industry, I am concerned that CAT/BPSS falls short in the area of requirements generation and collaboration with the Science and Technology (S&T) Directorate. It appears that the development and deployment of CAT/BPSS technology lacks two critical considerations: 1.) a thorough risk analysis of the threat scenarios that the technology addresses and its associated cost-benefit, and 2.) the necessary system requirements to achieve risk-based operational success.

I commend TSA's emphasis to move towards a more risk-based approach to airport security, so I am puzzled by the apparent lack of risk and cost-benefit analyses for the CAT/BPSS technology. My staff and I have requested several times that TSA provide us an analysis of the projected costs for the CAT/BPSS units, especially given that there is a planned large-scale acquisition as early as five months from now. TSA has provided neither cost projections nor cost threshold requirements for the technology. Secondly, while the technology is claimed to be part of a layered approach to airport security screening, we have not seen any risk analysis that supports the role of this technology in the overall security architecture. Specifically, the technology only detects

potentially fraudulent documents, and does little or nothing to link these potentially fraudulent documents to terrorist-related threats. CAT/BPSS provides no interconnectivity to other government threat databases, provides no protection against falsification of IDs at the issuing source, and provides limited assurance that damaged or misprinted, but valid IDs (or boarding passes) can be correctly processed by the system.

I also commend TSA for its use of systems engineering principles in developing a set of operational requirements for the CAT/BPSS technology. However, I remain deeply concerned, due to the lack of risk-based analyses, that some key requirements have been excluded. Examples of missing requirements that have been observed include:

- No requirement for interconnectivity to other security systems within or external to the TSA system architecture
- No requirement for false alarm rates. Since only detection rates and throughput rates are specified, the 'threshold settings' will likely be set to such a low rate that potential threats will pass through undetected.
- No requirement for human factors. How do we avoid false confidence by the TSOs as they see repeated readings of 'PASS' by the automated screens? How do we ensure that the technology does not distract from the TSOs' ability to observe passengers for behavioral cues?
- No requirement for phasing in the technology, based on risk and effectiveness. The acquisition plans call for a bulk procurement of 1400 CAT/BPSS units for deployment at 50% of all lanes at all airports. Based on prior TSA technology experiences, it would seem that a more phased, risk-based procurement and implementation would be prudent.

As you are aware, I intend to hold a hearing on CAT/BPSS next week. This hearing will provide TSA the opportunity to clarify the issues and offer solutions for a path forward. In preparation for this hearing, **I request that TSA provide the following information by June 15, 2012:**

- Projected costs of CAT/BPSS, including per-unit costs and projected lifecycle costs
- Requirements documents for CAT/BPSS
- Risk analyses conducted on CAT/BPSS, including quantitative assessments of the terrorist-based threats that CAT/BPSS will address, and its role in the overall TSA security system architecture
- Delineation of the ways in which the S&T Directorate has been engaged and what its expert feedback has been. At my visit to the TSIF on May 30, 2012, the CAT/BPSS program team affirmed there was some level of collaboration with S&T. Since that time, the S&T Directorate has denied having a role in CAT/BPSS development.

Thank you for your prompt and personal attention to this matter. I appreciate your continuing efforts to secure the nation's transportation systems and look forward to working with you to improve TSA's performance in carrying out its critical mission.

Sincerely,

A handwritten signature in black ink that reads "Mike Rogers". The signature is written in a cursive, flowing style.

Mike Rogers
Chairman
Subcommittee on Transportation Security



SECURITY MANUFACTURERS COALITION
ACC 

March 26, 2012

Honorable Mike Rogers
Chairman
House Subcommittee on Transportation Security
H2-175 Ford House Office Building
Washington, DC 20515

Sent Via Electronic Mail

Dear Chairman Rogers:

The members of the Security Manufacturers Coalition thank you for the opportunity to offer suggestions for improving the Transportation Security Administration (TSA) procurement process. The TSA has recently implemented some improvements to their process, and we are pleased to report that to date the agency has been receptive to working with the coalition to identify meaningful reforms. We will keep you and the Subcommittee apprised of our progress in these discussions.

The industry recommendations are intended to help ensure that qualified security technologies are deployed in the most cost-effective and timely manner possible. The suggestions included in the attached document were provided by the coalition member companies. The coalition members have also been invited to provide your office with specific recommendations or case studies at their discretion.

We look forward to working with you to affect needed improvements to the procurement process and enhance security within our borders and around the world.

Sincerely,



T.J. Schulz
Director, Security Manufacturers Coalition

Enclosure



RECOMMENDED CHANGES TO THE TSA PROCUREMENT PROCESS

Summary

The Transportation Security Administration (TSA) can foster the procurement of best performing technology by better defining requirements through enhanced industry days, Requests for Information (RFIs), and post industry meetings to better understand technical goals and challenges associated with meeting potential requirements. Once requirements are better defined, TSA should implement a process that establishes predictable milestones based on technical performance for meeting procurement eligibility.

Pre-RFP Release

1) Improve the Establishment of Requirements

The TSA has taken steps to improve communication with the industry. Additional steps can be taken to enhance engagement with the OEMs to ensure that requirements are both realistic and understandable. Establishing requirements is frequently the most difficult phase of an acquisition because the government must know what technology is mature enough to be integrated into products. Inadequate requirements have resulted in multiple amendments to Requests for Proposals (RFPs) or extended the time required to review and respond to inquiries.

TSA should continue to advance efforts to establish open, transparent and up-front requirements and specifications for technology testing and development. This can be accomplished by allowing OEMs to have greater input to the specifications prior to or at the initiation of the procurement process. Enhanced communication with the vendor community will result in the development of the correct requirements before the release of an RFP.

A) Use Requests for Information (RFIs):

- The RFI should state the operational need and mission and the desired result. TSA should provide detail on how it envisions the use of this equipment or technology. Along with defining what capabilities are desired, the RFI should constrain the problem and outline what technologies are not acceptable.

- Beware of basing RFIs on previous acquisitions and incorporating many of the requirements from existing systems. While the requirements may be legitimate, they often specify exact sizes, data storage requirements, and some software feature that are not driven by the operational need, but their historical use. Use a database to establish and derive specifications, and do not place specifications in an RFI or RFP if they are not needed, many specifications are simply carried over from old tenders.
- B) Improve Industry Days: Effective industry days can provide an information forum that helps TSA understand the current state of technology, and communicate its needs to industry. This will be exceptionally helpful in clarifying requirements and the intended concept of operations, and provide insight to equipment availability and intended timing for deployment.
- Use general meetings (not associated with a specific RFI) to stay current on technology and new equipment capabilities, and, and inform industry of initiatives and priorities.
 - Include one-on-one meetings at industry days. Different formats and lengths can be adapted, and time can be limited by advance scheduling. One-on-one meetings allow vendors to ask questions they do not feel comfortable stating in a group, or discuss proprietary information. TSA can take advantage of the exchange and determine if any of the information should be shared, and send a follow up summary of the one on one meetings as well.
 - Ensure staff is thoroughly prepared and knows the requirements. TSA should have the right people available to answer questions and representatives should be adequately prepared to discuss requirements for specific tenders, and know the derivation of requirements when they are published, even as draft.
 - Provide relevant and comprehensive information in the industry day publication so vendors can effectively prepare, providing a more efficient exchange.
- 2) Include consistent, or clearer, definitions of evaluation criteria in the requests for proposals.
- 3) Implement the multi-year budget planning efforts contained in the FY 2012 Omnibus Appropriations bill (P.L. 112-74) to provide transparency into the acquisition, refresh and sustainment for passenger screening technologies within the TSA.
- 4) Reduce the bureaucracy in procurements. Every purchase has a contracting officer, a contracts administrator, a COTAR, a PM, the Chief engineer, and then several layers of portfolio management, and the TSL. As a result, it is often unclear to industry who has responsibility over the program. These parties should function as a team for each procurement action, with the Program Manager in the lead.

At the same time, the contracting officer generally requires that all communications and questions go through them; however, the contracting officer usually will not have the requisite technical knowledge and may not be capable of answering the question. Vendors are also unable to meet with the contracting officer or anyone associated with the acquisition.

- Eliminate the layers of management, and appoint a program manager with enough technical ability to understand the systems and management ability to make a decision and push programs through.

- Provide the capability to have personal meetings between the industry and the procurement team – the PM, CO, COTAR, etc., to make sure the vendor fully understands the requirements and the contracting officer can play a supportive role. The meeting should include a representative from OSC to provide technical expertise.

Testing Process

Efforts should be undertaken to streamline the testing process for technology. It currently takes a minimum of 18 months to get a product certified. The testing process is cumbersome and many contain requirements that are not germane to the operational effectiveness of the technology. Currently the TSL does the testing in-house, and it takes weeks to coordinate the release of results. At the same time, there is little coordination between testing done by TSL and TSIF, and there is much redundancy and delay in the parallel processes. There are no interim steps to identify minor issues which could easily be changed but are not identified until the end of the testing cycle. This unnecessarily lengthens and adds complexity and cost to the program. During testing, these minor issues can often be rectified quickly, instead of waiting until the end of the process and requiring the vendor to repeat the entire segment.

TSA (and DHS) should develop a process that relies on clearly defined series of lab, field, and operational tests on a rolling schedule to allow for new technologies to be tested and validated frequently. An open schedule will encourage technology companies to invest in new research with more assurance that their investment will be vetted and potential acquired by TSA and DHS.

- 1) DHS should implement a consistent five step process for meeting procurement eligibility.
 - a) Submittal of a Qualified Data Package (QDP) – Once DHS has put forth a technology specification, a company submits their QDP which states that their technology meets the procurement specification.
 - b) Qualified Readiness Test (QRT) – Once the QDP has been submitted and approved, a company submits their technology for QRT. Under this process, the technology is tested and feedback is provided by DHS regarding the possibility of meeting the specifications.
 - c) Qualified Testing – Once feedback from the QRT has been taken into consideration and appropriate technology changes have been made, a company submits its technology for lab testing.
 - d) OT&E – After lab testing is completed and a technology meets the required specifications, the technology is deployed for field testing.
 - e) Eligible for Procurement – Technology is eligible for deployment once it is determined that it operates successfully in the field.

These steps are a rolling process. Any time a company believes it has a technology that meets the specifications, the company may submit their technology and progress through the process.

- 2) Provide consistent and timely communication back to OEMs regarding deficiencies and the establishment of a reasonable schedule to allow for improvements during the test cycle.

- 3) Emphasize TSIF's role as facilitating process optimization, and enhance coordination between the TSL and TSIF testing processes to eliminate redundancy and delay.
- 4) Institute hard limits on the testing time government has to meet as part of the procurement process, and provide more accountability on government to provide GFI that is needed to support vendor testing and development.
- 5) Consider incorporating "trial lanes" or "development lanes" at the checkpoint or checked baggage area to provide real data to vendors and the opportunity to improve equipment to meet operational requirements at TSA.
- 6) Explore authorizing third-party vendors to provide testing on a pay-as-you go basis. This can enable concurrent rather than sequential testing of multiple vendor submittals, further shortening the implementation of new technology.

Post Award:

- 1) Hold post-award meetings with industry.
- 2) Take steps to implement more reasonable delivery schedules post award.

End.

The Security Manufacturers Coalition serves as the united voice representing companies that manufacture security screening technology. Organized under the Airport Consultants Council (ACC), the Coalition focuses on aviation and intermodal security issues in the U.S. and globally. The Coalition advocates for the specific interests of its member companies relating to funding and acquisitions, technology research programs, and international regulations and standards.



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 16, 2012

Honorable John S. Pistole
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Administrator Pistole:

We are deeply troubled by the recent revelations outlined in a Department of Homeland Security Inspector General (DHS IG) report entitled “Transportation Security Administration’s Efforts to Identify and Track Security Breaches at Our Nation’s Airports.” The report indicated that ten years after 9/11, the Transportation Security Administration (TSA) is still struggling to identify and track security breaches at our Nation’s airports. The Subcommittee on Transportation Security convened a hearing today to discuss this matter, and quite frankly, we were extremely frustrated with the testimony the Subcommittee received outlining TSA’s ambiguous plans to respond to these revelations.

The DHS IG looked at six of the 28 Category X airports across the United States from January 2010 through May 2011. According to the IG’s findings, TSA staff is responsible for reporting all security incidents that occur at airports to an internal TSA reporting system called Performance and Results Information System (PARIS).¹ However, the audit showed that system to be woefully underutilized.

Over a 15-month period of time, only 42% of security breaches that inspectors reviewed were ever reported in PARIS.² Additionally, the IG could identify corrective action being taken by TSA in just 53% of all incidents.³ These statistics are unacceptable, and after the testimony given in today’s hearing, clearly reflect a systemic problem.

Acting Inspector General Charles Edwards also testified that his office identified a number of badges issued with one or more instances of omissions or inaccuracies of key applicant data used for vetting, such as STA status, birthdates or birthplaces. Many of the omissions or inaccuracies pertained to critical information used for vetting. For example, one applicant was listed as having three active badges at three different airports. The applications for

¹ OIG-12-80, Transportation Security Administration’s Efforts to Identify and Track Security Breaches at Our Nation’s Airports, 3.

² Ibid, 10.

³ Ibid, 12.

this individual reflected three different places of birth: the United Kingdom, Ukraine, and the United States. With inaccurate information on place of birth, TSA was unable to accurately vet the applicant, yet the three airports issued the requested badges. When asked, the Inspector General confirmed that TSA's database of information was 'worthless' and further stated that TSA concurred with this assessment. These findings are alarming, and need to be immediately addressed.

The IG's report issued two specific recommendations 1) TSA must refine its definition of a security breach so that it is clearly understood, and 2) TSA must develop a comprehensive oversight program to ensure that security breaches are accurately reported and that TSA consistently takes actions to correct vulnerabilities resulting from security breaches. TSA concurred with these two findings, and while TSA indicated in today's testimony that they are taking steps to address these problems, no concrete timetable was given. As was stated during the hearing, it does not matter what definition of a breach you use; the fact is that TSA Headquarters needs to be made aware when someone is able to get through to the secure side of an airport when he or she does not follow proper procedures.

While we have been lucky so far, and the security breaches that have occurred have not lead to more serious incidents, it only takes one time. And with a huge financial cost to taxpayers, we frankly expect better from those who are responsible for securing our aviation system. It is extremely concerning that it takes an Inspector General report for TSA to address the fact that it does not have a clearly articulated definition of what constitutes a security breach, when preventing security breaches is a fundamental component of the agency's core mission. The American people deserve better.

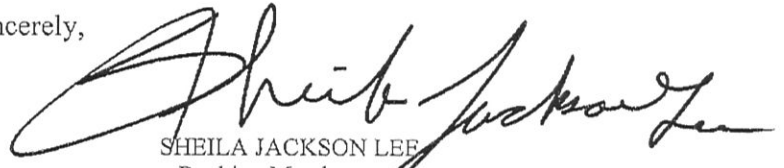
Given TSA acknowledgement of these vulnerabilities, and the severe consequences that any individual breach could cause, we ask that TSA address both of the Inspector General's recommendations within 30 days. If TSA is not able to address these vulnerabilities, in that timeframe with its own internal resources, then it should seek help from the private sector. Regardless of how the work is completed, these recommendations address critical security vulnerabilities and must be addressed within 30 days. There is no excuse for not reporting, tracking, and correcting breaches. Let us be clear: it is incumbent upon your agency to fix these management problems regardless of your ambitions for a Universal Rule or any other regulatory changes down the road.

Due to the urgent nature of this matter, we would appreciate a written response within 7 days outlining how TSA will address the IG's two recommendations within 30 days. We look forward to continue working with you to improve TSA's performance in carrying out its critical mission.



MIKE D. ROGERS
Chairman
Subcommittee on Transportation Security

Sincerely,



SHEILA JACKSON LEE
Ranking Member
Subcommittee on Transportation Security



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

March 27, 2012

The Honorable Janet Napolitano
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Dear Secretary Napolitano:

We write to indicate our strong interest in the Department of Homeland Security's (DHS) rulemaking regarding Aircraft Repair Station Security becoming final in this calendar year.

As you know, Congress mandated DHS to promulgate these rules in the 2003 Vision 100- Century of Aviation Reauthorization Act (P.L. 108 – 176 Section 611). Congress revisited the issue in the 2007 Implementing the Recommendations of the 9/11 Commission Act (P.L. 110 – 53 Section 1616), to again require the agency to complete this rulemaking. The 2007 law also barred the Federal Aviation Administration (FAA) from issuing an operating certificate to a new foreign repair station applicant if DHS failed to implement this rule within 240 days. As a result, since August of 2008, the FAA has been unable to certify new foreign repair stations, creating competitiveness issues for aviation manufacturers seeking to compete in foreign markets and weakening FAA's global safety leadership. It is unacceptable that a rulemaking first mandated in 2003 is still pending today.

Based on a recent letter from Administrator John Pistole to industry stakeholders, we understand that the rule will not be finalized until December 2012. As the leadership of the Subcommittee with jurisdiction over the agency, we respectfully request that you expedite this rulemaking before that date. If the current promised date is not met, we believe that alternative means such as orders or security directives to meet security requirements must be advanced. While we understand the myriad of issues facing both Transportation Security Administration and DHS, completing this rulemaking in 2012 must be accomplished to enhance security and address the economic consequences to industry, which have resulted from government inaction.

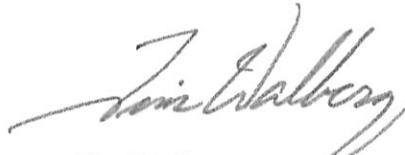
Recently, Assistant Administrator John Sammon and others from TSA recently briefed us on the status of this rulemaking and we request that you regularly brief the Subcommittee on your progress. In addition, Mr. Sammon indicated TSA's support for legislative action to ensure certification of new foreign repair stations can resume if the rulemaking encounters further delay.

Thank you in advance for your review of our request and we look forward to your prompt response.

Sincerely,



Mike Rogers
Chairman
Subcommittee on Transportation Security



Tim Walberg
Member of Congress
Subcommittee on Transportation Security



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515
November 30, 2011

Honorable John S. Pistole
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Administrator Pistole:

In the challenging economic environment we face, it is critical to ensure that taxpayer dollars are being used in the most effective way possible, especially as it relates to our security. The Transportation Security Administration (TSA) has purchased and deployed hundreds of pieces of screening technology throughout the United States; however, TSA also allocates resources to many storage facilities to store equipment that is not currently in use.

We understand that TSA's technology needs change and that equipment can require repairs, but we are concerned that the American taxpayer may be paying to store equipment that will never be used in U.S. airports and will sit in storage indefinitely. We applaud TSA's efforts to reach agreements with foreign airports to use equipment to conduct screening for U.S.-bound flights. Unfortunately, these agreements exist in very limited cases. For most of its unused equipment, TSA continues to maintain numerous storage facilities throughout the country.

The Subcommittee on Transportation Security recently held a series of hearings focusing on improvements that can be made to TSA's technology procurement process. We want to ensure that taxpayer dollars are used efficiently, and are not being squandered on equipment that does not meet our operational needs, and then further wasted on storage facilities for that equipment.

Specifically, we respectfully request your response to the following questions by no later than December 12, 2011:

1. Where are the locations of TSA's storage facilities?
2. What is the annual cost of maintaining each of these individual storage facilities?
3. How many pieces and what type of equipment is currently in each of these facilities?
4. What is the operational value of the unused equipment?
5. Approximately how much money was spent to purchase the equipment?
6. Does all of the equipment in storage meet TSA's current security standards? If not, what percentage of the equipment in storage does not meet current standards?

7. What steps is TSA taking to improve and enhance the international equipment loan program?

Thank you for your prompt and personal attention to this request. Should you have questions, please contact Amanda Parikh with the Committee on Homeland Security Staff at (202) 226-8417.



Mike Rogers
Chairman
Subcommittee on Transportation Security

Sincerely,



R. Blake Farenthold
Member
Committee on Homeland
Security



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

October 14, 2011

Honorable John S. Pistole
Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Administrator Pistole:

I am writing to express my strong concerns regarding the September 27, 2011 ruling of the United States Court of Federal Claims in the case of FirstLine Transportation Security, Inc. (FirstLine), vs. The United States and Akal Security, Inc.

According to the ruling, the Court found that TSA's acquisitions process in this case was fundamentally flawed and must be set-aside. The Court specifically found that TSA awarded a Screening Partnership Program (SPP) contract to Akal Security to provide screening services at Kansas City International Airport in Kansas City, Missouri (MCI) despite the fact that its proposal was found to be significantly weaker overall than the proposal submitted by FirstLine, the contractor currently providing screening services at MCI. The Court specifically cited, among other criticisms, that:

- The best-value analysis performed by TSA's Source Selection Evaluation Board was both irrational and inconsistent with the evaluation criteria set forth in the Request for Proposal (RFP), and that the award to Akal Security was fundamentally unfair; and
- TSA not only ignored the dramatic difference in the number of strengths assigned to each of the proposals, but that it also irrationally minimized the significant differences between the proposals.

These findings call into question TSA's ability to make responsible contracting decisions, and whether taxpayer dollars were unnecessarily wasted in this process. Moreover, I am deeply concerned that a contractor was selected to screen passengers and help secure our aviation system despite TSA's own admission, according to the Court's ruling, that it would pose more operational risk and require governmental intervention. This type of poor judgment is unacceptable in my view, considering the continued threats to aviation security. I hope you will agree that TSA runs the unnecessary risk of endangering travelers and causing serious economic

damage by narrowly focusing on the cost advantages of one SPP proposal over another, rather than a true comparison in the ability to carry out security screening services.

SPP was authorized by Congress in 2001 and it has been a successful program over the last ten years. TSA has repeatedly certified that all private screeners perform at or above the level of Transportation Security Officers. Kansas City International Airport is one of the largest U.S. airports participating in SPP, first entering the program in 2002. I am concerned that, particularly in light of your decision in January to limit expansion of this program, TSA's improper contracting decision involving one of the programs largest airports and one of its highest performing private screening companies seems to indicate that TSA is not serious about the program and would rather see it fail than succeed. I continue to feel strongly that the private sector has an important role to play in security and must be properly leveraged, not forced out of the process in favor of a larger federal workforce.

While it is my sincere hope that the poor handling of this RFP resulted from human error and was not intentionally flawed, I am requesting your full cooperation and assistance to bring greater transparency to the rationale behind this decision and ensure that any deficiencies are addressed quickly. **I request that you provide by no later than October 24, 2011, copies of all documents and communications created by or in the possession of TSA that pertain to the RFP issued by TSA on April 2, 2010, and the subsequent related contract award decision made on March 17, 2011, to perform SPP contract screening services at the Kansas City International Airport.** The terms "documents" and "communications" are intended to mean all records including, but not limited to, files, reports, analysis, assessments, memoranda, notes, and presentations, in all forms of media, including emails or other electronic communications, and including any archived materials.

Additionally, as Chairman of the Subcommittee on Transportation Security, I intend to hold a hearing on SPP and the handling of the MCI contract in the coming weeks, and I respectfully request that you provide testimony at this hearing. I understand that TSA has already made a decision to issue a new RFP for the MCI contract following the Court's ruling. I urge you to postpone any action on this RFP until the Subcommittee can complete a review of the documents requested and conduct necessary oversight of TSA's acquisitions process in support of a robust SPP and proper use of taxpayer dollars.

Thank you for your prompt and personal attention to this matter. I appreciate your continuing efforts to secure the nation's transportation systems and look forward to working with you to improve TSA's performance in carrying out its critical mission.

Sincerely,



Mike Rogers
Chairman
Subcommittee on Transportation Security



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

March 11, 2011

The Honorable John S. Pistole
Administrator
Transportation Security Administration
Arlington, VA

Dear Administrator Pistole:

I am very concerned by the release of information today by the Transportation Security Administration (TSA) regarding inaccurate contractor reporting concerning test results for x-ray technologies deployed by TSA in our nation's airports. Such x-ray technologies include backscatter advanced imaging technology systems which have been the subject of great public debate. I understand that TSA has conducted its own evaluations of all backscatter AIT systems and that the radiation emission measurements are well within applicable safety standards. However, I am deeply troubled by TSA's lack of oversight and management of the continued testing of these technologies.

TSA has the responsibility to ensure to the traveling public that these technologies are evaluated on a regular basis and to ensure that all machines are safe. Accordingly, I ask that TSA audit all contractor reports on a quarterly basis and provide those audits to the Committee on Homeland Security's Subcommittee on Transportation Security. I also request that TSA immediately retain an independent third-party auditor to verify that the x-ray technologies deployed in the nation's airports are safe.

I look forward to personally discussing this matter further next week. Thank you for your attention to this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Mike Rogers", written over the word "Sincerely,".

Mike Rogers
Chairman
Subcommittee on Transportation Security



One Hundred Twelfth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

February 17, 2011

Mr. John Sammon
Assistant Administrator
Office of Transportation Sector Network Management
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Assistant Administrator Sammon:

Thank you for taking the time to meet with me on January 20, 2011, to discuss the Office of Transportation Sector Network Management's (TSNM) efforts to secure our nation's transportation systems. Your briefing was thoughtful and informative and I appreciate your time. I look forward to future conversations with you regarding TSNM and its efforts to continually improve transportation security.

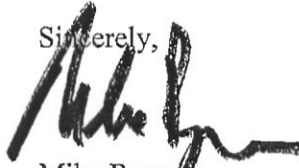
As a follow-up to our meeting, I would appreciate your response to the questions below. Pursuant to Rules X and XI of the House of Representatives, I request that you respond to the following questions no later than Wednesday, March 16, 2011:

1. Following the thwarted air cargo attack in October 2010, TSA implemented air cargo security directives that placed restrictions on cargo shipped from Yemen and Somalia and prohibited high-risk cargo on passenger airplanes. Can you provide an update on TSA's air cargo security initiatives in Yemen?
2. Shipping companies such as UPS and FedEx have cooperated with TSA to improve security in the aftermath of the thwarted Yemen attack. Can you further define what role, both financially and structurally, private industry currently plays and will continue to play in maintaining, developing and enforcing air cargo security standards?
3. You stated that TSA would conduct a security assessment of the key rail tunnels. Can you provide details as to the schedule for those assessments, how many tunnels are being assessed, and what criteria were used to select those tunnels?
4. Can you provide an update on the Registered Traveler Program? What are TSA's plans for developing and promoting this program?

5. How quickly and to what extent is TSA planning to integrate canine explosives detection teams into passenger screening operations at airports?
6. In FY 2011, the operational cap under the Transportation Security Grant Program is reduced to 10%. This change will limit the amount of funding available from TSGP to fund operational costs incurred by transit agencies and local law enforcement involved with security for mass transit systems. How will the reduction in the operational cap in the Transportation Security Grant Program (TSGP) affect mass transit security? What mass transit agency security programs will be affected by the decrease in operational funding?
7. TSA is currently conducting a pilot with Greyhound to improve and enhance passenger and baggage screening for weapons and explosives. Please provide more detail regarding the passenger screening pilot being conducted by Greyhound in Houston, TX and Los Angeles, CA. Are there plans for additional pilots in other cities?

Thank you for your prompt and personal attention to this request. Should you have questions, please contact Amanda Halpern with the Committee on Homeland Security Majority Staff at (202) 226-8417. I look forward to continue working with you to ensure the security of our nation's transportation systems.

Sincerely,



Mike Rogers
Chairman
Subcommittee on Transportation Security