Reason

May 2003

A Risk-based Airport Security Policy

By Robert W. Poole, Jr. with George Passantino
Project Director: Robert W. Poole, Jr.

POLICY STUDY 308

Reason Public Policy Institute

A division of the Los Angeles-based Reason Foundation, Reason Public Policy Institute is a public-policy think tank promoting choice, competition, and a dynamic market economy as the foundation for human dignity and progress. Reason produces rigorous, peer-reviewed research and directly engages the policy process, seeking strategies that emphasize cooperation, flexibility, local knowledge, and results. Through practical and innovative approaches to complex problems, Reason changes the way people think about issues and promotes policies that allow and encourage individuals and voluntary institutions to flourish.

Reason Foundation

Reason Foundation is a national research and education organization that explores and promotes the twin values of rationality and freedom as the basic underpinnings of a good society. Since 1978, the Los Angeles-based Foundation has provided practical public-policy research, analysis, and commentary based upon principles of individual liberty and responsibility, limited government, and market competition. REASON is the nation's monthly magazine of "free minds and free markets." It covers politics, culture, and ideas through a provocative mix of news, analysis, commentary, and reviews.

Reason Foundation is a tax-exempt organization as defined under IRS code 501(c)(3). Reason Foundation neither seeks nor accepts government funding, and is supported by individual, foundation, and corporate contributions. Nothing appearing in this document is to be construed as necessarily representing the views of Reason Foundation or its trustees, or as an attempt to aid or hinder the passage of any bill before any legislative body.

Policy Study No. 308

A Risk-based Airport Security Policy

BY ROBERT W. POOLE, JR. WITH GEORGE PASSANTINO

Executive Summary

Today's U.S. airport security policy rests on a fallacious proposition. By applying equal screening resources to all passengers and all bags, the system *acts as if* security officials believe that every passenger and every bag is equally likely to be a threat. This premise wastes limited security resources on low-risk passengers and bags, thereby devoting less resources to higher-risk passengers and bags. In addition, this approach has created a "hassle factor" at airports that drives away airline passengers. Credible estimates put the lost airline business due to this factor in the vicinity of $3 billion per year.

A more intelligent approach to airport security is to apportion security resources to passengers and baggage in proportion to estimated risk—just as law enforcement agencies do in other circumstances, ranging from the stalking of public figures to family violence. Risk-based airport security would mean a reduced focus on finding *bad objects* and an increased focus on identifying potentially *bad people*—those most worthy of additional scrutiny. Screening resources would then be applied in accordance with a passenger's risk category. This report shows how a risk-based system can be implemented without posing a threat to the privacy of air travelers.

Risk-based principles are already used by the federal government with respect to border-crossing, where a number of programs (such as INSPASS and NEXUS) permit travelers to volunteer for pre-clearance, enabling them to bypass long lines when they actually pass through border facilities. Likewise, in the cargo area, "known-shipper" programs represent additional uses of risk-based decision-making. Overseas airports, in Israel and Europe, use risk-based techniques such as passenger profiling and trusted traveler programs to sort passengers into different risk groups for differential processing at the airport. Seen against this broad background, it is the security approach used for passengers and bags at U.S. airports that is out of step.

This report reviews the two key tools needed for a risk-based security model for U.S. airports. The first is a system for pre-clearing a subset of low-risk passengers, who can then receive expedited processing at airports. The current term for this is a Registered Traveler program. The second is a system for selecting out high-risk passengers for extra scrutiny. Our proposed Risk Screening System (RSS) would replace the current, flawed Computer-Assisted Passenger Prescreening System (CAPPS).

With tools of this sort in place, both passenger and baggage screening can be redesigned to reduce delays and to redirect screening resources to where they are most needed. All checked bags of high-risk passengers would be screened by the most expensive (and generally slowest) explosive detection systems, but only a random fraction of other bags would be processed by those machines, rather than faster, less costly machines. All baggage processing would be carried out in secure baggage areas, away from crowded passenger lobbies for both safety and security reasons.

Under this risk-based approach, all passengers would be thoroughly screened at the security checkpoints at the entrances of concourses. This would eliminate last minute screening at the boarding gate. To make this possible, information from the RSS must be available at passenger screening checkpoints. Hence, all passengers must obtain boarding passes from either a ticket counter or an e-ticket kiosk in the lobby. The screening checkpoints must be redesigned to provide for (1) expedited lines for Registered Travelers, and (2) additional positions at which those selected by RSS can undergo additional screening.

Both the Registered Traveler program and the Risk Screening System could pose troubling privacy issues, depending on how they are designed and used. The Registered Traveler program requires a membership database, but it will be more acceptable to passengers if that database is administered by one or more private sector firms, interfacing with Transportation Security Administration (TSA) for the actual clearance decision and with individual airlines for customer interactions.

For the risk-screening function, TSA's proposed CAPPS-II would create a massive, intrusive database on the personal and financial details of air travelers. This is far more than required for the task of identifying high-risk travelers for enhanced scrutiny at airports. Our proposed RSS, by contrast, would rely on the information already contained in airline reservation systems (which could have singled out a small subset of air travelers including all of the 9/11 hijackers). Creation of TSA's proposed Aviation Security Screening Records database should be forbidden by Congress.

The shift of TSA into a new Homeland Security Department offers a good opportunity to rethink the past year's over-emphasis on passenger airline security, at the expense of numerous other vulnerabilities in U.S. transportation, let alone other vital infrastructure. Shifting to a risk-based approach to airport security should be an integral part of that rethinking.

Table of Contents

Part I

Introduction: Today's Flawed Airport Security Paradigm

In response to the terrorist attack of Sept. 11, 2001, Congress felt itself under intense pressure to act quickly to strengthen airport security. With the best of intentions, it created a new federal agency—the Transportation Security Administration (TSA)—and imposed on it a series of mandates and deadlines. Implicit in both the legislation and its interpretation by the TSA is a basic fallacy—that all passengers and bags should receive equal scrutiny. Policies based on this idea have made airports less secure than they might be; imposed huge monetary costs on airports, passengers, and taxpayers; and created a "hassle factor" that has contributed to massive losses for air carriers.

A. The Equal Resources Fallacy

Current airport security policy is based largely on the idea that the government must treat all people equally. That means treating every passenger alike and every bag alike. In other words, the same amount and extent of airport security resources must be devoted to every passenger. Every one of them must remove their laptops from their briefcases—no matter how much or how little is known about them. Every one of them must be subject to random pat-downs and shoe removal—regardless of their age or physical condition.

Implicit in this policy is the assumption that every passenger is equally likely to be a terrorist and that every bag is equally likely to contain explosives or other harmful materials. Likewise, each and every checked bag must eventually be sent through a $1 million Explosive Detection System (EDS) machine, regardless of the identity and history of that bag's owner. Each and every carry-on bag must have its nail scissors removed, no matter how much we may know about its owner. Even airline pilots, to whose judgment we entrust entire plane-loads of people, must have these same procedures applied to them.

There are many things wrong with the equal resources model. Most important, it can actually decrease airport security. At any given time, only so many resources (say $6 billion/year) will be available for airport security, given the numerous other U.S. security concerns, let alone all the other functions of government. If we divide that total sum (in this case, $6 billion) equally among all 600 million passengers who fly within the Untied States each year, that's $10 per passenger. Does it really make sense to spend the limited funds in this averaged way, rather than spending a larger sum on that subset of passengers most likely to be bent on causing harm?

An alternate approach might seek to divide the entire set of airline passengers into three groups:

1. Those about whom a great deal is known, all of it consistent with that person not being a threat;
2. Those about whom very little is known, and what is known is correlated with known risk factors; and
3. Everyone else.

If there were a reliable way of sorting passengers into those three groups, it would make sense to spend much less than $10 per person on those in the first group and much more than $10 per passenger on those in the second group. Perhaps only the third group should have the average amount, $10, spent on each. The point of spending several times $10 on each passenger in the second group is that finding the "needle in a haystack" is difficult and costly. That effort is more likely to succeed if more resources are devoted to it. That might mean, for example, requiring people in the second group to submit to back-scatter X-ray screening—the technology that can see through clothing and detect plastic explosives and ceramic knives concealed on (or inside) the person's body. Neither cost nor privacy concerns justifies subjecting all travelers to this screening procedure. But information putting some passengers in the high-risk category might well do so.

This is an illustration of how shifting from the equal resources premise could significantly increase airport security. It would permit significantly more of our limited security dollars to be targeted to where they would do the most good. In the process, it might mean that we would not need to spend as large a fraction of our always-limited security resources just on airports—because we would be spending those airport funds in a much smarter way. A large airport might need only 15 or 20 of the million-dollar-apiece EDS machines (rather than 40 or 50) if the bags of those in the first group were not all required to be scanned by EDS.

The equal resources fallacy was criticized by Rafi Ron, the former head of security for Israel's Ben Gurion Airport, in testimony before the House Aviation Subcommittee. Ron told the Subcommittee members that it would be too time consuming to search every piece of luggage and every traveler to make sure there were no weapons or explosives. "Without the ability to take an intelligent decision on where to invest our effort, we end up wasting our attention on the 'low-risk' passengers," he said.[1]

B. The Hassle Factor

Today's airport security policies, grounded in the equal resources fallacy and the random selection fallacy, are less effective than would be a policy focusing greater resources on higher-risk passengers and their bags. But in addition to using limited security resources badly, these policies are also harming the aviation industry. The increased unpleasantness of air travel has contributed to the current record-high airline losses, as travelers cut back on trips. The general term for this phenomenon is the "hassle factor."

While some consider the evidence for this phenomenon to be merely anecdotal, statistical data have been accumulating for some time. A March-April 2002 survey of corporate travel buyers, conducted by the Business Travel Coalition, probed what factors accounted for reduced business flying in 2002. For those who had reduced air travel by 25 percent or more, "airport security delays and hassles were the clear leaders, with 51 percent ranking them first."[2] More recently, a survey of business travelers commissioned by Orbitz for the Travel Business Roundtable in August 2002, found the following:

- Nearly four out of every five (79 percent) of frequent business travelers have received heightened security screening (i.e., a "pat down" or removal of shoes).

- More than one in ten travelers (11 percent) have canceled their flights or fly less frequently because of the hassles of airport security.
- Thirty-one percent of female business travelers who have reduced their level of flying because of the hassles of security have done so because of the personal "intrusion from security." By contrast, of male business travelers who have reduced their level of travel, only 4 percent cited the intrusion of security as the reason.

A survey by Delta Airlines of its frequent flyers found that nearly 25 percent cited the hassle factor for not flying. Extrapolating this result to all airlines, the Air Transport Association estimated that the hassle factor would cost airlines $3.8 billion in revenue in 2002,[3] though a subsequent ATA briefing paper put the 2002 impact at $2.5 billion.[4] Regardless of the exact number, nearly all experts agree that the hassle factor is real and that it has reduced the extent of airline travel.

Part 2

Introduction to Risk-based Decision-making

A. Disproportionate Fear, Disproportionate Response

Thousands of people die every year in auto accidents, yet we willingly drive to work with little regard for the danger. By contrast, the events of a single day, when teams of terrorists crashed two planes into the World Trade Center, another into the Pentagon, and a fourth plane into a Pennsylvania field, turned our sense of safety and our world upside down.

As a result of this fear, the federal government enacted a series of hasty mandates and restrictions to improve the security of air travel—ranging from the prohibition of nail scissors and mandated explosive screening for all baggage to the federalization of passenger and baggage screening—despite evidence that these reforms would likely not have prevented the September 11th attacks. Using rage, fear, and brutality as their weapons, the terrorists could have seized the planes with wooden pencils or a leather belt. They carried no explosives. The quality of the passenger screening staff had little bearing on the situation because the terrorists violated no rules and carried no illegal items onto the planes.

The tragic result of this fear is that we make ourselves vulnerable—not safer. According to an estimate based on RAND Corporation studies, the total cost of implementing just the 100 percent explosives screening mandate may be as much as $12 billion, more than three times the entire budget of the Federal Bureau of Investigation.[5] Further, this country has embarked on creating the world's largest security agency, composed of 66,000 federal airport security personnel. Only by strategically allocating resources can we build a world of relative security. Devoting so much to a single risk, such as scanning all airline bags for explosives, makes little sense.

Relative to the spectrum of risks we face as a free and open society, security overall operates on a shoestring budget. We simply can't afford to put explosive detection systems or National Guardsmen at the entrances of all hospitals, football stadiums, schools, malls, and skyscrapers where the potential for disaster is as great as at airports. Even if we devoted the entire budget of the federal government to preventing terrorism, we could not seal off every point of vulnerability.

Best-selling author, Gavin de Becker, an expert on violence prevention and risk management, put the challenge of airport security after 9/11 in perspective in his most recent book, *Fear Less*:

> *I believe with substantial certainty that the hijacking of commercial jets the way it has been done in the past is just that: a thing of the past…Regular citizens now constitute the lowest-tech and most effective element of security on airliners. All the meticulous searches, National Guardsmen, X-ray machines, questions at ticket counters, metal detectors, double checking of IDs, and confiscating nail clippers don't equal the effectiveness of a few passengers willing to act decisively when someone tries to gain unauthorized access to the cockpit. The 9/11 murderers likely did not know they had committed the hijackings to end all hijackings. But that's what happened as Americans viewed and re-viewed history's most effective training video—produced by the terrorists themselves.*[6]

Still, aviation security is essential because the risks are significant. Jet hijackings once carried the potential for death of, at most, a few hundred people. We now know that the cost can be much higher, killing thousands of people. As such, appropriate security measures must be enacted to meet this threat.
De Becker is perhaps best known for his innovative work in addressing the following question: *How can we best allocate a limited set of resources against a virtually limitless supply of risks?* Large city police departments confront this question when they receive too many domestic violence calls for their detectives to investigate. Major corporations and universities confront similar questions. The U.S. Secret Service, the U.S. Court Police, the U.S. Capitol Police, state police agencies protecting governors, and any number of other law enforcement agencies confront this same challenge. There are simply too many potential threats against the lives of the people they protect to respond to all potential threats equally.

This is the nature of the threat in aviation security as well. Millions of people walk through airports each and every day of the year; millions of bags move down the conveyor belts. Any one of them *could* be a terrorist or a bomb. Given the similarities to other situations where threats exceed available resources, aviation security policy can draw many lessons from those with experience in the practice of what could be called *risk-based decision-making*.

These protectors of governors, school children, and victims of family violence all recognize, with full knowledge, that they cannot possibly address all risks equally so they focus their resources on those that present the highest stakes and the greatest dangers. They also recognize that doing so makes their job more effective and the people they are protecting safer. Unfortunately, these lessons have not been applied to airport security. In order to do so, policymakers must first understand the concept of risk-based decision-making.

B. Principles of Risk-based Decision-making

The fundamental characteristic of risk-based decision-making is the ranking of risks along a quantifiable scale—typically expressed numerically like a credit report score (which is, itself, a risk-based decision-making tool). Once risk levels are assessed, resources—such as law enforcement intervention, investigation, or additional passenger screening—are applied in measures proportional to the risk level. High-level risks receive extensive scrutiny via technology and other means. Mid-level risks also receive scrutiny, though not as much as the high-risk cases. Most critically, the least serious risks receive the least attention—intentionally so.

While there are numerous risk-based decision systems in use, de Becker's MOSAIC has received attention for its use in high-stakes cases. The MOSAIC method involves establishing areas of inquiry, or questions,

that experts and statistical studies have determined to be most valuable to an assessment. Users of the method input answers to numerous questions, and analytical software captures, weighs, and interprets key variables. These variables, organized together, can be compared to past cases with known outcomes, i.e., cases that escalated and cases that did not escalate. For example, to assess the level of urgency of any given domestic violence complaint, a police detective answers numerous questions on various subjects, including the presence of children in the home, recent financial distress, the history of abuse, alcohol use by the abuser, pet abuse, homicide, and suicide threats. Even data points that are not individually predictive, when combined and weighed, can assist assessors in making case management decisions.

Risk-based decision-making is not the same as racial or ethnic profiling. Taking all individuals of Middle Eastern descent and focusing all efforts on scrutinizing them would be as ineffective as confiscating nail clippers. Timothy McVeigh, Ted Kaczynski, Eric Harris, and others like them demonstrate that hazards can come from any ethnic group.

Instead, risk-based decision-making is based on the interplay of numerous variables, none individually being necessary or sufficient to trigger a high-risk score. For instance, somebody may have several late payments to his cable company but he will still have a very low credit risk (or high creditworthiness) score if he is Bill Gates or Warren Buffet.

C. Risk-based Decision-making and Aviation Security

Applying the risk-based decision-making paradigm to preventing terrorist attacks on commercial aircraft would require two primary decisions:

- Reducing the focus on finding bad objects (100 percent baggage searches, etc.) and increasing the focus on identifying people most worthy of additional scrutiny.
- Developing a system that processes people and bags based on the risk category in which they fall.

Already, a mechanism exists that could serve as a starting point for the development of a “scoring” system. Used to assess potential risks of passengers, airlines apply a tool known as CAPPS (computer-assisted passenger pre-screening), which is, itself, a risk-measurement tool. The disconnect in current practice is that the security system *after* that point does not effectively differentiate between high- and low-risk passengers. With the 100 percent explosives screening mandate, all bags receive the same scrutiny. This means, automatically, that the scrutiny must be less effective than it would be if fewer (the most likely to be dangerous) bags were to be given more intensive scrutiny. Likewise, all passengers must wait in the same lines and receive the same scrutiny (metal detectors, random shoe removal, frisking, etc.). Minutes spent scrutinizing the lowest-risk passengers are minutes that could be applied to higher risk passengers, to greater effect.

Part 3

Current Uses of Risk-based Systems in Transportation

Despite defenses of the equal resources approach from the top levels of the U.S. Department of Transportation, the federal government already applies risk-based approaches in a number of transportation areas. While its only application in airport security is CAPPS, systems based on dividing people and cargo into different categories are widely used elsewhere in U.S. transportation. And risk-based systems are applied more consistently in airport security in a number of other nations. The brief review in this section suggests that current U.S. airport security policy is out of step with widely accepted practices in transportation.

A. Current U.S. Programs

Both before and after 9/11, the principle of risk-based security was used in various areas of U.S. transportation. In aviation, CAPPS was already in use to decide which air travelers fit a high-risk profile and should therefore have their checked luggage screened by X-ray or explosive detection systems. Thus, the pre-9/11 airport security policy—as limited as it was, given the then-current perception of the threat level—conformed to the risk-based model.

The stated reason for not adopting the risk-based model across the board for airport security is the principle that government must treat all citizens (and by implication here, all users of airports and air transportation) equally. To do anything other than this would be considered discriminatory. Yet in any number of ways existing U.S. policy treats different parties differently in transportation, following the general principle that streamlined treatment or processing can be provided to a person or cargo if significantly more (benign) information is known about the party in question.

The Appendix describes six current examples of this principle. Two of these—the Immigration & Naturalization Service Passenger Accelerated Service System (INSPASS) and the Advance Passenger Information System (APIS)—involve quicker processing of arriving international airline passengers about whom information has been provided in advance. Two other programs involve pre-clearance of people for speedier border crossings on land—NEXUS for the U.S.-Canadian border and SENTRI for the U.S.-Mexican border. And another INS program, called PAL, allows frequent drivers on I-5 in Southern California to use an express lane at the San Clemente Checkpoint.

In addition, the basic security model being used in both air cargo and surface cargo (both pre- and post-9/11) is called "known shipper." Its basic principle is that instead of requiring every container or other piece of cargo to be inspected (as with checked airline baggage), those that are tendered by "known shippers" do not have to be screened by explosive detection systems, except on a random, spot-check basis.

In every case, the underlying principle is the same. Low-risk people and goods, about whom sufficient information is known, do not need intensive scrutiny at the time and place of travel. It is a waste of resources to deal with them as if they were either high-risk or of unknown risk. Even worse, doing so would represent a diversion of always-limited security resources that would be better devoted to more intense scrutiny of higher-risk people and goods. By the same token, people and goods about whom there is reason to be suspicious, or about whom too little is known to make a judgment, should be processed differently, with a greater use of resources.

These principles are widely used in transportation, and are the foundation of much post-9/11 security policy. The glaring exception is the current equal resources treatment of airline passengers and baggage, under the provisions laid down in the Aviation & Transportation Security Act of 2001.

B. Risk-based Airport Passenger Processing Overseas

1. Israel's Trusted Traveler Program

Israel is well-known for having the world's most rigorous airport security system. It is founded solidly on a risk-based approach. In comparing the Israeli system with ours, former Israeli Air Force chief intelligence officer Jeff Feldschuh says that the current U.S. model, in which searching for dangerous objects is primary, must be inverted, to put its primary focus on potentially dangerous people. This requires sorting passengers into groups, who receive different airport processing based on risk level.

At Ben Gurion Airport in Tel Aviv, a trusted traveler program has become an integral element of that process. Begun in 1996 in response to chronically long lines at the airport, the system was developed by a U.S. company, EDS. Any Israeli citizen may apply for membership, which involves a background check and in-person interview, plus an annual fee of $20-25. Those who are accepted have their hand geometry measured and encoded on a machine-readable identity card. Upon arriving at the airport, members proceed to one of 21 kiosks with hand scanners, where their identity is verified. This enables them to proceed through less cumbersome security check-in procedures. EDS reports that members' check-in time averages 15 minutes, as compared with two hours for other passengers. As of late 2001, about 15 percent of the passengers at Ben Gurion were members of the trusted traveler program.[7]

2. Amsterdam Schiphol Airport's Privium

In October 2001, the commercially oriented Amsterdam Schiphol Airport launched a one-year trial of a more limited biometrically based system for speeding up one element of passenger processing. One year later, the system had close to 5,000 paid-up members.[8] Privium uses iris scans instead of hand geometry measurements for its biometric identifier. Potential members (who must hold European Union passports) go through a 15-minute enrollment process, which includes a check of the validity of their passport, a check against a European police database, and an iris scan. Membership costs 99 euros per year. Members in

Privium Basic are allowed to use special automated lanes at border control and separate and faster passenger security screening lines. Privium Plus, in cooperation with participating airlines, provides separate check-in counters and priority parking at Schiphol Airport.[9]

The system was developed by Schiphol Group and Dutch security technology company Joh.Enschede Security Solutions. The technology is also being tested at several Canadian airports, at Frankfurt, and at New York's JFK International Terminal 4, which is run by Schiphol Group. In April 2002 IBM announced a joint venture with Schiphol Group to sell and install the technology worldwide.[10]

3. S-Travel

The International Air Transport Association (IATA), along with other aviation organizations, is working with a company called SITA to test another form of trusted traveler program called S-Travel. Like the Israeli and Dutch programs, it will also use a biometric smart card to verify that the passenger presenting the card is the same person who has passed the initial background check and been accepted into the program. An initial six-month trial was due to start in fall 2002 at two European airports, most likely Milan and Zürich. In addition to being used to expedite passenger security screening, the same technology will also be used for employee access control. Initial funding for the project is being provided by the European Commission and the Swiss Office for Education and Science.[11]

C. Risk-based Baggage Processing in Europe

European airports are committed by a European Union Transport Council decision to implement 100 percent checked-baggage screening at more than 400 airports in 38 nations by Dec. 31, 2003..[12] This follows the eight-year implementation of the same goal by U.K. airports, which was completed there in 1998. However, European airports are not deploying the very expensive ($1 million apiece) EDS machines mandated by Congress in the 2001 Aviation and Transportation Security Act (ATSA) to screen all bags. Rather, European airports typically make use of multi-tier systems in which the EDS machines make up the final tier. That final tier has two distinct uses. The first is to resolve suspicious readings made by the faster and less costly first or second-tier automated X-ray machines (similar to those used for carry-on luggage). But the second use is to be the primary screening tool for high-risk passengers.

In other words, European practice with regard to checked-baggage screening is risk-based, as was U.S. practice prior to the passage of ATSA. In this nation, until recently the policy had been to use CAPPS to identify high-risk passengers, and to designate their checked luggage for explosive detection inspection. Where EDS machines were available, they were used for this purpose. Otherwise, either explosive-sniffing dogs, electronic trace detection, or manual bag-opening was used to check those bags. This continued to be U.S. practice in the months leading up to the ATSA deadline of Dec. 31, 2002, at which point every checked bag, regardless of the passenger's risk level, must be checked for explosives. Thus, ATSA represents a decisive step away from the risk-based approach that has been standard in this nation and that is still the policy in Europe, as that continent adopts a different kind of 100 percent baggage inspection.

Part 4

Overview of a U.S. Risk-based Airport Security System

As noted in Part 1, airport security under the Airport and Transportation Security Act of 2001 is based on an equal resources principle. All air travelers and all pieces of baggage are nominally treated equally. A risk-based system, by contrast, depends on sorting passengers and their bags into two or more risk groups, with screening resources applied to each group in proportion to its risk level.

Our proposal is that a risk-based U.S. system sort passengers into three basic groups: high-risk, low-risk, and everyone else. Thus, tools for carrying out this sorting process are essential. In this section, we discuss two such tools and then suggest how the application of these tools would lead to significant changes in the processing of both passengers and baggage.

A. Separating High-risk Passengers

A rudimentary tool for separating high-risk passengers already exists and is in use—but the tool and its use are flawed. The system is called CAPPS (Computer Assisted Passenger Prescreening System). CAPPS makes use of information provided by passengers when they make their reservations and purchase their tickets. It uses a set of algorithms to determine patterns believed to be correlated with terrorism. The full list of those factors is (properly) classified, but it is widely known that among the factors are paying cash, purchasing a one-way ticket, and making reservations at the last minute. CAPPS assigns numerical points to the many factors analyzed, resulting in a total point score for each passenger.

CAPPS was developed by Northwest Airlines, with FAA financial assistance, and was first deployed by that airline in 1996. The following year, the White House Commission on Aviation Safety and Security (the Gore Commission) recommended that CAPPS be used by all airlines. Other airlines began using CAPPS in 1998, but the FAA's 1999 rules for making use of CAPPS limited that use to determining which passengers' checked luggage should be screened for explosives. The FAA barred airlines from using information from CAPPS to subject passengers themselves to personal searches and questioning (termed "manual screening"), because that use "has been criticized by persons who perceived it as discriminating against citizens on the basis of race, color, or national origin."[13] Limiting CAPPS to the selection of checked luggage for explosives-screening can be done without the passenger's knowledge, thereby minimizing complaints about bias. This restriction meant that potentially high-risk passengers flagged by CAPPS were not, therefore, singled out for more intensive screening at passenger checkpoints or boarding gates, either of their carry-on

baggage or of their persons. Accordingly, the 9/11 hijackers, nine of whom had been flagged by CAPPS, were not searched at the checkpoints.

Two changes were made to CAPPS following the events of 9/11. First, the weighing criteria in the algorithms were modified, based on new information. The other change was to expand the use of CAPPS to all passengers, whether or not they have checked luggage, and to subject those "selectees" to additional screening at the boarding gate. Those passengers' boarding passes are marked to indicate that they should be pulled aside during the boarding process for manual inspection of their carry-on bags, shoes, etc. Because the criteria used for this purpose are the same ones originally developed to keep potential explosive-filled checked suitcases off planes, the system ends up selecting large numbers of people in short-haul markets (inter-island Hawaii flights, east coast Boston-New York-Washington shuttles, Texas triangle flights) who make short day trips. Many of these people make last-minute reservations, may pay cash due to the low fare, and often purchase only one-way tickets. In some of these cases, more than 50 percent of passengers are selectees requiring gate screening.

CAPPS also selects some passengers for random screening (which accounts for only a small portion of those receiving manual inspection at the gate). In addition, when a flight ends up with very few CAPPS-designated selectees, the gate screeners select additional passengers for manual inspection, to maintain a desired workload level.

The greatest deficiency in CAPPS is that it does not provide real-time access to federal watch lists of potential high-risk passengers—contrary to numerous media reports contending that this change was implemented post-9/11. Instead, the pre-9/11 system continues, under which the FBI and INS provide periodic additions (and deletions) of individual watch list names, by fax or email. In the case of INS, these manual updates are sent to the Air Transport Association (which represents the major air carriers) and to INS chiefs at individual airports. The FBI sends its manual updates to the FAA, which sends them to individual airlines.[14]

Airlines have proposed several ways of improving the dissemination of this information. For example, they recommended that the FBI and INS merge their information, send it to the TSA, and have the latter send it to each airline electronically, but so far that proposal has not been implemented. The Airlines Reporting Corp. (a travel agency clearinghouse) has volunteered the use of its detailed database of advance-booking information to the TSA so that the previous travel patterns of watch list people could be analyzed, but this offer has not been accepted.[15]

In addition, the FBI "watch list" itself is flawed for these purposes. The list includes the names of many people who have done nothing wrong. Attorney General Ashcroft has acknowledged that this list is simply used to identify people with whom law enforcement wants to talk. Airlines many times notify the authorities of an "exact match" only to be told that the authorities don't want to take the time to interview the person.[16]

There is a critical need for a computer-based watch list of persons who are possible threats to airline security. Besides simply including such a person's name, however, it must include enough identifying information to eliminate confusion over identity. In addition, there should be an associated action for each person—i.e., what should be done if that person is found to be purchasing an airline ticket (e.g., be questioned, be arrested, etc.).

Thus, today's CAPPS (and the way it is used) is a flawed tool for separating out high-risk passengers. It fails to incorporate real-time access to meaningful federal watch list data, and it does not make use of travel-industry databases for checking the prior behavior of watch list persons. Its selection criteria are poorly suited to its current use in screening all passengers. And today's system leaves the more intensive screening of the carry-on bags and persons of selectees until the last minute, at the boarding gate, instead of performing this function at the passenger screening checkpoints at the entrance to the boarding concourses.

The TSA is developing a successor system to be known as CAPPS II. A draft plan for upgrading airport security, prepared by PWC Consulting, EDS Inc., and A.T. Kearney, calls for making the data from CAPPS II available at checkpoints as well as ticket counters.[17] Another planned change will be to check each passenger record against relevant federal databases in real time. But the most recent TSA proposal for CAPPS II goes far beyond CAPPS by proposing the creation of a massive database—called Aviation Security Screening Records—on all air travelers.[18] In addition to making use of the passenger name record (PNR) information in airline reservation systems, the system would use data-mining techniques to probe a variety of private and government databases to generate information about those "deemed to pose a possible risk to transportation or national security." Information about such people would be stored to up to 50 years. Such comprehensive data-mining and record-keeping raise obvious privacy and civil liberties concerns, which have been pointed out in some detail by the American Civil Liberties Union and the Electronic Privacy Information Center in their responses to TSA's Federal Register notice. We address those issues in Part 5.

Some of those who developed the Israeli approach to airport security have suggested that algorithms based on past behavior are insufficient to reliably identify high-risk passengers. On this view, CAPPS should be supplemented by computer-assisted "behavior profiling," i.e., the systematic observation of passenger behavior while at the airport, from curbside to boarding. One company with Israeli roots, Secant, proposes to "analyze how large numbers of people behave as they go through an airport. It would automate much of the analysis . . . and allow screeners to check off any suspicious behavior they see."[19] A benefit of this approach is that it would make it safer to eliminate what some call "silly searches," allowing resources to be better focused on those far more likely to be high-risk passengers. In November 2002, Massport, the parent agency of Boston's Logan Airport, announced that the airport had implemented behavior profiling, under the term "pattern recognition."[20]

In short, the current CAPPS is inadequate, but the currently proposed CAPPS II attempts to do too much, raising serious privacy concerns by probing the details of passengers' lives and circumstances. The alternative is a simpler Risk Screening System aimed solely at identifying high-risk passengers. It would (1) provide real-time access to all relevant watch lists, (2) use more sophisticated algorithms that are updated regularly to take into account new information on terrorist activities, and (3) make better use of airline and travel-agency databases that can provide past-travel histories of those on the watch lists. That system could perhaps be supplemented by real-time behavioral profiling at the airport, on the Israeli model.

B. Separating Low-risk Passengers

The counterpart of separating high-risk passengers from the mix is a system that can voluntarily separate low-risk passengers, who can be given less intensive scrutiny by airport security systems. This is the "trusted traveler" or "registered traveler" concept, the latter term preferred by the TSA's director, Admiral Loy. As

the General Accounting Office noted in a comprehensive review of the concept, "a Registered Traveler Program could potentially improve aviation security and more effectively target resources."[21]

The logic of such a program is straightforward. Certain people today have already been cleared via rigorous processes and judged to be worthy of various kinds of trust. Airline flight crews, especially cockpit crews, have the power to turn an airliner into a deadly guided missile. They need no hand-carried weapons to do so; hence, they must undergo a regimen of licensing and medical exams that gives us a high assurance that they can be trusted to fly these planes in the manner intended. A second obvious category of already-screened traveler is the large number of Americans who have gone through the extensive background checks needed to receive government security clearances. If these people are to be trusted with life-and-death military secrets, they ought to be trusted to not sabotage the airliners on which they fly.

A Registered Traveler program simply extends this logic to an additional set of people, who make the voluntary choice that in exchange for less hassle at airports, they are willing to undergo a civilian version of security clearance, unconnected with government service. Many proposals have been made as to the criteria that should be met for issuance of such a clearance, and it is not our purpose here to get into the exact details. One proposed set of criteria was offered in a recent RAND report.[22] It suggests the following:

- An unexceptional National Agency Check;
- A fingerprint check against criminal and civil files;
- A verified, stable employment history;
- A record demonstrating firm community roots;
- A record of financial security with no unexplained deviations from typical patterns;
- A travel history consistent with occupational history; and
- An employer's statement of confidence.

In addition to the background check, such a program requires two other elements to be secure. One is a secure identification card. The person showing up at the airport claiming to be a Registered Traveler must demonstrate that he or she is the same person who was cleared by the background check. This can be done by the person presenting a card encoding biometric information unique to that person (fingerprints, hand geometry, iris scan, or face geometry). In order to be accepted for passenger processing as a Registered Traveler, the biometric information on the card must match a real-time measurement of the card-presenter's fingerprints, hand, iris, or face.

The other requirement is that the database of Registered Travelers would have to be kept secure. If the database could be hacked and a non-cleared person's name and particulars entered, then that person could show up at the airport with a counterfeit card (with correct biometric data) and be processed as if he or she were an actual Registered Traveler.

Such a system raises no privacy concerns, because it is voluntary. It could be operated as an adjunct to individual airlines' frequent flyer programs (though operating in accordance with uniform standards set forth by the TSA). Applicants would pay an initial fee to cover the costs of the background checking, and presumably an annual membership fee, as with current programs in Israel and The Netherlands (see Part 3). It would also be wise to require periodic re-clearance via a new background check.

One of the first detailed presentations of the concept for U.S. airports was made by aviation experts Michael Levine and Richard Golaszewski, whose basic argument was that rather than expending equal effort on screening every one of the two million enplaned passengers each day to find the needle in a haystack, it would make better sense to voluntarily screen frequent travelers before they show up at the airport.[23] The idea has subsequently been endorsed by airline CEOs, airport officials, former FAA Administrator Jane Garvey, Homeland Security director Tom Ridge, and most recently TSA director Admiral James Loy.

Northwest Airlines developed the first detailed proposal for testing the idea using airline employees. Director Ridge asked the Air Transport Association to develop a unified airline industry proposal to test the concept for both employees and a sample of frequent fliers. That proposal was submitted to the TSA in August 2002, and is still undergoing review.[24] It proposes a 90-day test involving 11 airports and 12 airlines (with a lead carrier at each participating airport or terminal). Registered Employees in the test would be airline employees who had passed the required airline employee background check and a criminal history background check. Employee participants would include pilots, flight attendants, corporate officials, and ground personnel. Registered Travelers in the test would be members of airline frequent flyer programs who volunteer to participate and who either (1) hold a federal security clearance, (2) hold a military clearance, (3) have passed one of several specified state or local background checks, or (4) have passed a National Agency check. The purposes of the test would include testing the biometric technology, measuring processing rates, gathering data on false positive/negative rates, and developing procedures for responding to alerts and technical malfunctions.

C. Implications for Passenger Processing

Let us now suppose that a Risk Screening System is in place to identify high-risk passengers and a Registered Traveler program is in place that does likewise for low-risk passengers. How would the experience of passengers at airports change, if the system took full advantage of risk-based principles?

The aim, as noted in Part 1, is to apply an average amount of screening to “ordinary” travelers, more thorough screening to high-risk travelers, and less detailed (at-airport) screening to Registered Travelers (who, by definition, have been pre-screened).

To begin with, there would still be security checkpoints at the entrance to concourses, to provide for basic screening of passengers and their carry-on luggage. But the idea would be to make that checkpoint area the last hurdle before boarding, ending the practice of gate screening. All security equipment and people could be stationed at an enlarged set of checkpoints, eliminating the worry, hassles, and indignities of gate screening for all passengers. Obviously, this means more rigorous access control to the “sterile” areas of airport terminals that are past the security checkpoints—but that needs to exist in any event.

The security checkpoints would be reconfigured to provide separate lanes for Registered Travelers and all others. Registered Traveler lanes would be reserved for those whose identity had been verified and boarding pass issued, either at the airline check-in counter or at a kiosk encountered prior to the checkpoint. Those accepted into these lanes (using their biometric card again) could traverse them quickly, without having to remove laptops from carry-on bags. They would also be permitted to carry pre-9/11 toiletries such as nail scissors in their carry-ons. They would still have to pass through a standard metal-detector and have their carry-on bags pass through a standard high-speed X-ray machine. And if the detector alarmed or a screener

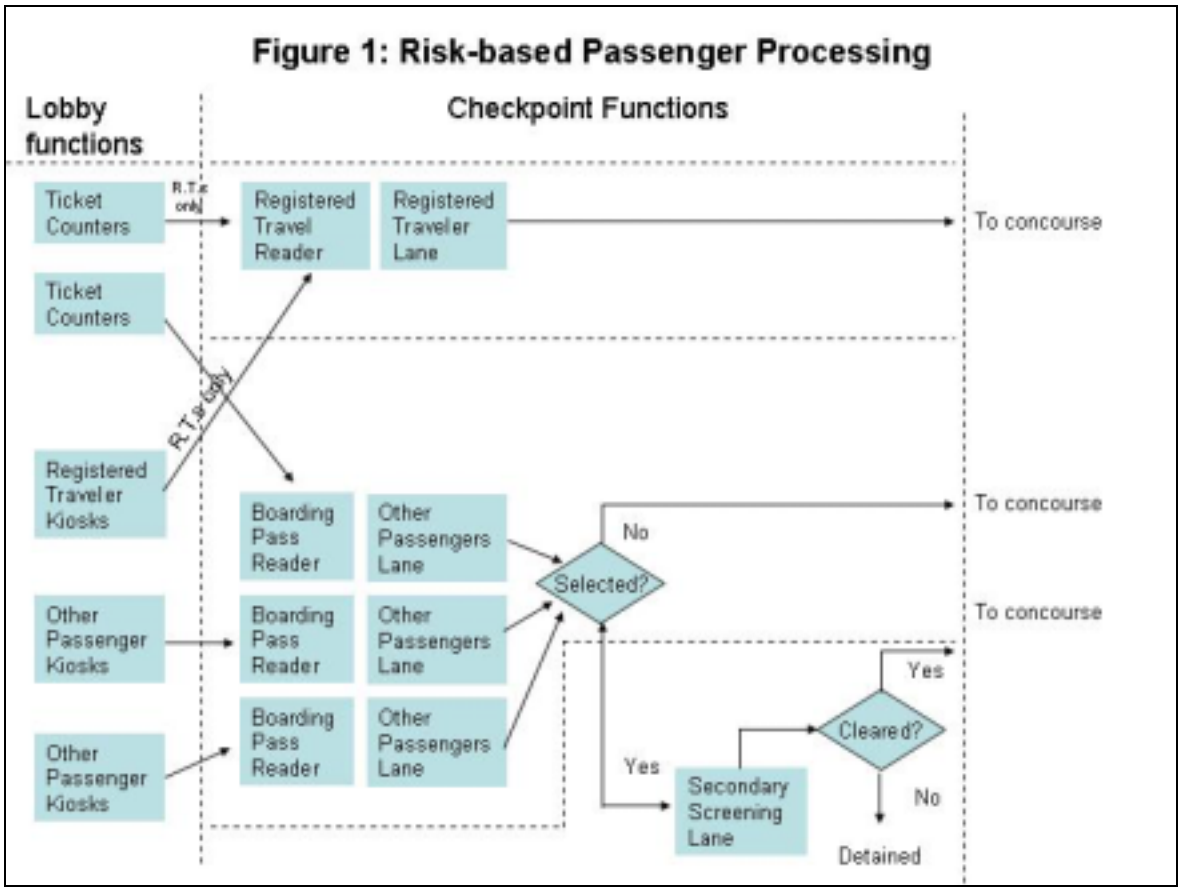
spotted a prohibited item on the X-ray, they would be subject to further scrutiny. Still, their passage through the special lanes would be, on average, much quicker than today. Everyone in the lane would be knowledgeable about the rules, so there would be significantly fewer delays. Not having to remove laptops would also save time.

All other passengers would pass through the regular checkpoint lanes. In order to make use of the RSS information in these lanes, all passengers would have to obtain a boarding pass prior to passing through security, either from the airline check-in counter or an e-ticket kiosk. Passengers whose boarding passes indicated (electronically) that they were selectees would, after exiting the initial checkpoint, be directed to an additional lane where they would pass through a back-scatter X-ray machine to identify any prohibited items under their clothing or concealed in body cavities. And their carry-ons would be subjected to trace-detection examination at this point, as a standard procedure.

Non-selectee boarding pass-holders (i.e., everyone else) would go only through the regular lanes, whose technology and procedures would be essentially the same as today's standard TSA model. The benefit to these passengers from the new system would be (1) shorter lines because the low-risk passengers have been diverted to other lines, and (2) the elimination of further checks at the boarding gate. Once past the checkpoint, they would be finished with security.

A risk-based approach to passenger processing would require several changes at airport terminals. There would need to be a large number of airline kiosks to issue boarding passes to e-ticket holders, since no passengers would be permitted through the screening checkpoints without a boarding pass. (At some airports where multiple carriers use a checkpoint, there may be a need for common use self-service kiosks, for which standards have recently been developed by the International Air Transport Association.) Separate kiosks would need to be provided for Registered Travelers, equipped to verify the biometric information on their cards. The checkpoint area would have to be expanded, to provide the new lanes for Registered Travelers. At larger airports, some lanes would have to be switchable between Registered and ordinary traveler usage, so as to cope with changing levels of demand for the two types of lane. Additional screening equipment would need to be installed past the regular checkpoints for high-risk passengers, in particular the back-scatter X-ray systems. These changes would require that more total space be available for checkpoints at each concourse.

This risk-based approach to passenger processing is illustrated in Figure 1.



D. Implications for Baggage Processing

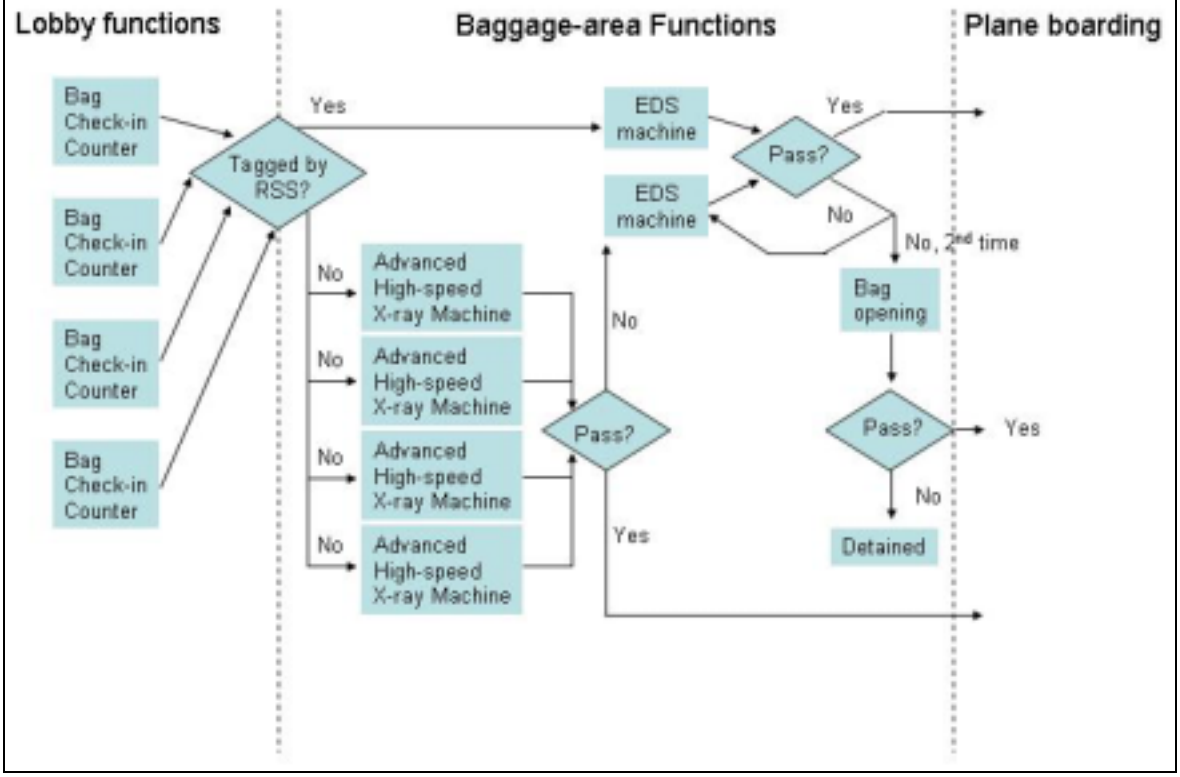
How would the processing of checked bags be changed by the shift to a risk-based system? Given the new reality of global terrorism, it makes sense to continue two policies that were adopted following 9/11: positive passenger-bag matching and 100 percent screening of checked bags for explosives. But a risk-based approach would permit the latter requirement to be done in a more effective manner, as is being done in Europe today.

Checked-baggage screening would be done via a several-tier baggage system, away from ticket lobbies. The ticket lobby is the wrong place in which to examine bags for explosives, especially when a fraction of bags must be opened. Most security experts agree that such inspections should be done in a separate location away from large concentrations of passengers. The most suitable location is the secure baggage-processing facilities, which need to be redesigned to handle new equipment and a revised flow of bags.

The first tier, as in Europe, would consist of advanced automated X-ray systems with processing rates of 1,000 or more bags per hour. TSA currently cannot use such systems for checked baggage screening due to the congressional mandate for EDS, but Congress nonetheless approves the use of high-speed X-ray for screening carry-on bags at passenger checkpoints. This is a meaningless distinction. A terrorist willing to commit suicide can carry on board sufficient explosives to bring down a plane in a carry-on bag. The same state-of-the-art high-speed X-ray systems should be used for both screening carry-on bags and for first-tier screening of checked bags.

All checked bags (except those tagged by RSS) would be processed via high-speed X-ray, to meet the 100 percent screening requirement. Bags exiting from this first-tier screening would take one of two paths. If the bag triggered an alarm, it would be routed automatically to a slower and more expensive tier-two machine (such as EDS or its successor), for a more detailed inspection. Bags cleared by the second tier would proceed to the plane-loading process. Any bag alarming on tier two, along with bags originally tagged by RSS, would go through a third tier of processing, such as a second pass through a tier-two device. Any bag triggering an alarm on a tier-three inspection would be opened for manual inspection in a secure location. This process is depicted in Figure 2.

Figure 2: Risk-based Baggage Processing



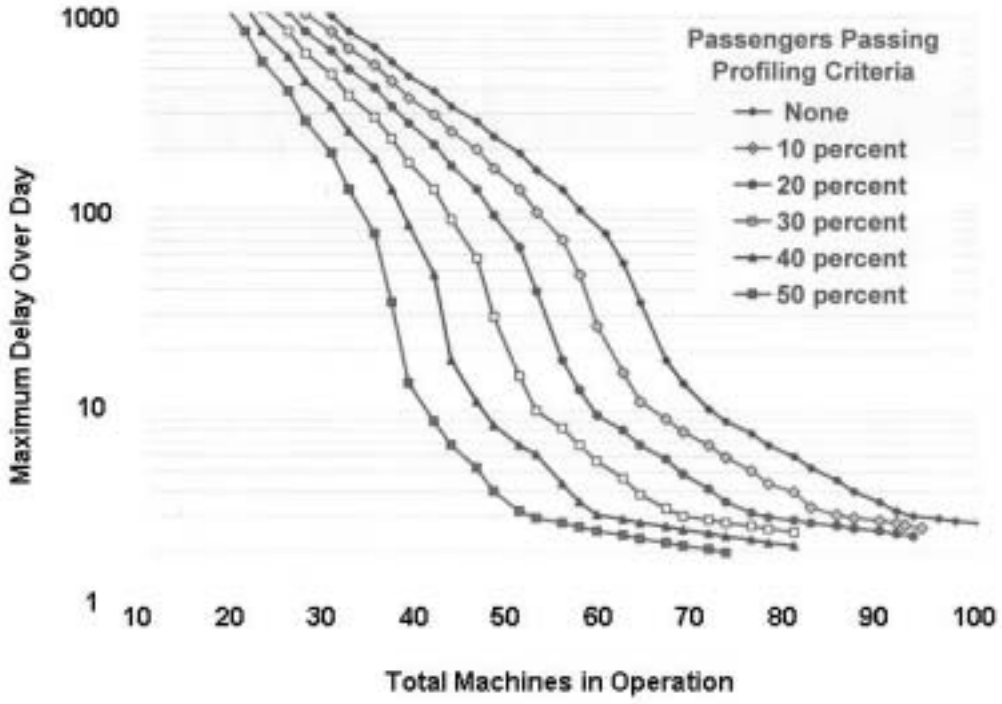
Many European airport policies call for the passenger to be summoned, so that he or she can be present at the time the bag is opened. There are two reasons for this policy. First, for liability reasons, most airlines wish to minimize claims that items were stolen from their bags in the event that the bag is opened during baggage processing, and the presence of the passenger as an observer should minimize such claims. Second, if the bag does contain an explosive device, the passenger must be located for questioning and possible arrest, and should not be allowed to board the plane.

The implications of this approach to checked-baggage processing would be dramatic. The massive numbers of lobby-based electronic trace detection (ETD) machines now used by the TSA would be unnecessary, and ticket lobbies could be restored to their original purpose. In addition, the upwards of 6,000 EDS machines[25] implied by the congressional mandate of 100 percent inspection of all bags by this technology could be dramatically scaled back. An in-line baggage system based on high-speed X-ray machines supplemented by

EDS and ETD (or their successors) would cost significantly less and take significantly less space than the systems now being planned by the TSA and its contractor, Boeing.

A recent RAND briefing paper makes quantitative estimates of the extent to which a risk-based approach would reduce the number of bag-screening machines required.[26] Figure 3 presents results based on conditions projected for DFW Airport in 2010, with about 90,000 checked bags per day. It presumes a two-tier baggage processing system, with the number on the horizontal axis being the total number of machines needed. The vertical axis is the maximum scanning delay. For example, if we want to keep that delay to 10 minutes or less, and if none of the bags are excluded from screening, the number of machines needed is close to 70. At the other extreme, if 50 percent of the bags are excluded because they are checked in by Registered Travelers, the number of machines is reduced to about 35. In other words, the analysis shows that the number of baggage inspection machines needed is roughly proportional to the number of bags to be screened—which can be reduced significantly via a risk-based system design.

Figure 3:Reducing Number of Bags to Be Scanned Significantly Lowers Maximum Delays



Source: RAND Corporation

Part 5

Issues with a Risk-based System

While there is much to be said in favor of a risk-based approach to airport security, this approach has raised a number of concerns among knowledgeable people—both those concerned with security and those concerned with privacy and individual liberty. In this section, we examine the principal concerns.

A. Privacy Issues

The most important set of concerns relates to the tension between security and privacy. Groups such as the American Civil Liberties Union and the Electronic Privacy Information Center have criticized both Registered Traveler and CAPPS-II proposals, seeing both as posing serious threats to privacy and liberty. The greatest fear is that in the name of combating terrorism, the federal government will create a massive database on everyone who travels by air, greatly infringing on everyone's privacy.

These are very legitimate concerns. There are definitely trade-offs involved, and in this discussion we will attempt to set forth guidelines that can give Americans the benefits of a risk-based approach (greater resources devoted to potential threats, less hassle and wasted time for ordinary travelers) without major Big Brother intrusiveness into their lives.

1. Registered Traveler Program

The first point to keep in mind is that a program to pre-clear frequent travelers (i.e., Registered Traveler) is distinctly different from a program to single out high-risk travelers (something like a CAPPS-II). The former is a voluntary program in which each traveler makes an individual decision about whether it is worth it to him or her to disclose various personal and possibly financial details in order to obtain the benefits of membership in the program. This is no different, in principle, from the decision to apply for a mortgage or to apply for a security clearance in order to accept certain government or defense contractor jobs.

The ACLU's Barry Steinhardt has argued that a Registered Traveler program would be voluntary only in a nominal sense.[27] Because there are 70 million members of frequent flier programs, "They would all want a card that allowed them to escape the grueling security regime at today's airports . . . .Those denied the cards would be increasingly subjected to intrusive, humiliating, and time-consuming searches. In a short time, Americans would, for all practical purposes, be forced to acquire a card and to submit to whatever procedures are used to issue it."

Some clarification is needed before addressing the substance of this argument. First, most members of frequent flier programs belong to several, so the total number of *individuals* involved is probably more like 25 million than 70 million. Second, an unknown number of these members travel only a few times a year, but still like the idea of building up mileage to obtain free trips. They are much less likely to apply than regular business travelers. Third, Steinhardt's argument assumes travelers are divided into just two groups—trusted travelers and non-trusted travelers. Our proposal, like most others of the risk-based sort, posits at least three groups: Registered Travelers, ordinary travelers, and high-risk travelers. To sum up this clarification: the Registered Traveler approach is, in fact, applicable to a distinct subset of all air travelers, not to air travelers in general.

Fundamentally, Steinhardt's argument amounts to a rejection of the premise that responsible individuals can, and should be allowed to, make trade-offs about privacy versus convenience. In today's high-tech society, people make these kinds of trade-offs all the time:

- Do I apply for an electronic toll tag?
- Do I apply for a debit card?
- Do I apply for a home equity loan?

Each of these (and many other) decisions involves either a one-time or an ongoing loss of some degree of privacy—but always in exchange for a set of benefits. We presume that adults are competent to weigh these trade-offs for themselves, rather than having someone else decide for them that the costs outweigh the benefits.

Another substantive question is whether a Registered Traveler program would involve the creation of a massive government database, involving complete dossiers on every member. Obviously, just as each airline's frequent flier program must keep track of who is a member in good standing, and at what level, in order to provide the appropriate member services, so would a Registered Traveler program have to maintain at least a membership database, applicable to all airlines, so that a member could show up at any U.S. airport, flying on any airline, and able to be verified as a member and processed through security accordingly.

This process is quite similar to that carried out worldwide millions of times a day by major credit card networks such as Visa and MasterCard. They maintain huge databases on card holders, including records of all their purchases, payments, balances, etc. Their software looks for unusual patterns in purchases, as indicators of possible fraudulent use of a lost or stolen credit card; in such cases they call the card member to ask about the purchase. Most people are comfortable with the extent and nature of data collection and database usage by these service providers. Why? Obviously, one reason is the great convenience provided by a global system of credit extension and no-hassle purchases. But another reason is that such services are offered by private firms, as opposed to the government. When it comes to making trade-offs of privacy for convenience, most people are less worried about their personal information and buying patterns being in the hands of a commercial firm than in the hands of what they may see as a Big Brother government.

Although most current discussions of proposed Registered Traveler programs take it for granted that this will be a TSA program, privacy concerns suggest that serious consideration should be given to the Visa/MasterCard model. In other words, while TSA itself will make the ultimate "security clearance" decision, day-to-day operation and administration of the program could well be outsourced to one or more private sector service bureau firms, who would interface with both TSA and the individual airlines.

Another point to keep in mind is that a Registered Traveler membership database need not require maintaining a detailed dossier on each member. It is quite possible for the system, in carrying out its clearance function, to obtain transient access to numerous government and private sector databases but without compiling and saving detailed personal information. (This is how ATM systems operate on a global, not just national, basis.) The point, after all, is to verify the low-risk nature of the applicant, not to build a file for prosecution. And while the details of what factors are used to accept people into the program must remain classified (to prevent sleeper terrorists from being able to manipulate the system to gain membership), the extent of personal information retained about members should be disclosed. This information will be a factor in many people's decisions about whether or not to apply for membership.

2. Selecting High-risk Passengers

Two main concerns have been raised about the other principal component of a risk-based system—the mechanism for identifying high-risk passengers. One concern is that any form of "profiling" is inherently wrong. The other is that such a system requires the creation of an intrusive database on all air travelers, without their consent.

On its extensive Web site on Air Travel Privacy, the Electronic Privacy Information Center posts the statement of the ACLU's Gregory Nojeim before the Gore Commission in 1996. Nojeim criticizes the basic idea of profiling as follows:

> *Reduced to its essentials, a 'profile' is a stereotype. It is a proxy for real evidence, but a profile is not a legitimate substitute for real evidence. It is rather a speculative means of predicting conduct—in this case criminal conduct . . . . From a civil liberties perspective, profiles are notoriously overbroad. Profiling violates the first principle . . .it permits treatment of passengers as potential criminals in the absence of facts specific to them that suggest they are likely to engage in criminal activity.*[28]

Nojeim goes on to say, "There is no substitute for evidence as a basis for suspicion. . . . When safety is a concern, time and money should not be barriers." But as anyone familiar with economics knows, resources are always limited, forcing choices to be made in the allocation of resources. And anyone familiar with law enforcement knows that such work always makes use of some form of educated guesses, based on experience and judgment, to help direct police activity to one set of suspects rather than all possible suspects. The question is not profiling or no profiling; rather, it is legitimate versus illegitimate profiling.
Legal expert Robert Levy of the libertarian Cato Institute takes a more nuanced view of profiling, recognizing both the dangers and the potential usefulness of such practices. He sets forth three tests, as follows:[29]

- **First, how important is the objective of the profile?** Levy notes that profiling in the case of terrorism has much greater potential to save lives than in the case of ordinary criminals.
- **Second, how effective is the profile likely to be in stopping the dangerous act?** In reviewing the eight major terrorist attacks against the United States and its allies in the past 30 years, Levy notes the involvement of Muslim male extremists in seven of the eight, and suggests the potential legitimacy of profiling that would take such characteristics into account, among many other factors.
- **Third, what is the potential for abuse?** In this case, Levy suggests that ethnicity or national origin might "add materially to the predictive power of a terrorist profile," and hence may be justified, especially if it is used simply to limit the scope of investigations.

While a full discussion of both the factors that are legitimate to use in anti-terrorism profiling and the legality of various factors under current U.S. law is beyond the scope of this paper, there is good legal precedent for some form of profiling system of this sort. When sensitive factors such as ethnicity and national origin come up in this context, what needs to be remembered is that CAPPS-type algorithms use a multiplicity of factors in a complex weighing and scoring process. If such a system were to include national origin, for example, it would be but one of dozens of factors that, in combination, would produce a score for assigning a person to a risk category. It would never be used as a stand-alone decision factor.

The other privacy concern—at least about the CAPPS II system proposed by TSA—is the creation of a massive database on air travelers (to be known as Aviation Security Screening Records). While only Passenger Name Record (PNR) information from airline reservation systems would be collected for all passengers, and would be stored only until the completion of the flight, additional information would be collected and stored (for up to 50 years) on "individuals who are deemed to pose a possible risk to transportation or national security." It is not clear from the TSA's Federal Register notice whether those in this category would be only those who should be detained if and when they show up at the airport, or if it would include the much larger group of travelers who would be categorized as requiring secondary screening at the airport.

This is a good example of what the ACLU's Steinhardt calls "function creep." The original idea of CAPPS was to analyze information in passenger reservation systems to detect suspicious patterns. To this was added, post-9/11, a crude manual effort to cross-check this information with FBI and INS watch lists. From this has grown a grandiose Big Brother quest to assemble incredibly detailed information about the private lives of everyone who purchases an airline ticket. The most extreme version is a Defense Advance Research Projects Agency (DARPA) project called "Total Information Awareness,"[30] which some have called an "Airline Echelon"[31]—a reference to the massive National Security Administration operation which eavesdrops on voice and electronic communications. Unfortunately, what TSA has proposed comes uncomfortably close to doing that.

While TSA is absolutely correct to insist that the inner workings (e.g., algorithms and scoring factors) in any such system must be classified in order for the system not to be outwitted by terrorists, its basic design concept must become a matter of public debate—and congressional vetting. It is not at all clear that the benefits of this type of data-mining on the personal lives of all air travelers are worth the costs in loss of privacy. That is especially relevant when it is realized that intelligent use of just the information contained in airline reservation systems can quickly and inexpensively provide very sophisticated sorting out of suspicious travelers, based entirely on patterns.

The example described in the box below demonstrates the power of using just PNR data to identify a subset of higher-risk passengers. The analyst defined a "threat scenario" somewhat like that used in the 9/11 attacks and—without using any names, ethnic data, or nationality data—produced a list of a small number of individuals including those named as the 9/11 hijackers. In short, there is sufficient richness just in the PNR data to identify a relevant subset of potential high-risk travelers for further scrutiny at the airport.

It should also be remembered that a Risk Screening System based on PNR data would not be the only tool in a risk-based airport security system. The Registered Traveler program will take a significant fraction of air travelers out of the pool of those the system must be concerned with. A rigorous real-time system for accessing up-to-date and relevant watch lists would add additional power to this approach. And keeping an

element of randomness in both passenger screening and baggage screening (see below) will help to safeguard the system against being circumvented.

America's initial efforts to improve airport security have created a "hassle factor" (as discussed in Part 1) that is estimated by the airlines to be costing them $3 billion per year in lost revenue, due to some people opting not to fly. It's not clear what air travelers would think about a massive federal database about their personal lives, but if giving up that degree of privacy, involuntarily, becomes a requirement for flying, that may only add to the number of people who opt for other modes of travel.

The Richness of Passenger Reservations Data

This example illustrates the richness of information contained in passenger reservations systems. The idea is to use MOSAIC-like threat scenarios and analyst groups to determine search parameters.

This example, carried out by airline I.T. experts Airline Automation, Inc. in conjunction with airline industry analysis firm R.W. Mann & Company, Inc., used as a threat scenario the pattern exhibited by the 9/11 hijackers. Obviously, this is just one of many possible threat scenarios. For this case, the task was to search for instances of four or more people traveling one-way, on flights longer than 1500 miles, departing prior to 8:30 AM, booked in a premium class, and booked more than 10 days in advance.

This query was run on a pre-indexed set of 5,024,524 domestic reservations for the period Aug. 22, 2001 to Oct. 19, 2001, before and after the attacks of Sept. 11, 2001. Of these reservations, 902,463 involved one-way travel. The query resulted in 13 unique data records (sets of people fitting the pattern). This search located *each and every record of named hijackers*, as well as some other people. The search did not make use of passenger names. It was generated on a 700 mHz laptop computer in less than 30 seconds.

This example suggests that a standard "bit search" procedure be established, whereby airline reservation data could be checked against many threat scenarios. These scenarios, created by law enforcement/security officials, could be run continuously on all active airline reservation data. To test its feasibility, a bit database was created, containing 3,250,000 rows of data—more than all travelers combined for one day of flights worldwide. Forty-four parameters ("values") were created—factors about each reservation that can be answered yes or no (i.e., rendered as a one or a zero)—and which could be used to specify various threat scenarios. Some 22 identical patterns were "planted" in the database, to determine the time it would take to find them. This was accomplished in six seconds, again using a 700 mHz laptop PC.

The core capability required is to be able to retrieve such data from airline reservation systems, format the data into a useful and standard format, and pass the data to a risk assessment or threat scenario engine operating in a closed-loop feedback process with a group of threat assessment analysts. Their task is to generate threat scenarios and factors. Any threats identified can then be passed back to the system as potential high-risk passengers.

B. Security Concerns

Those whose concerns are primarily about security worry that a risk-based system would be vulnerable to subversion by diligent terrorists. One concern is that a terrorist might be able to stealthily obtain membership

in the low-risk group of travelers. The other concern is over terrorists being able to outwit the selection of high-risk travelers for special scrutiny. Both concerns are addressed below.

1. Gaining Access to the Registered Traveler Group

Former TSA head John Magaw opposed the Registered Traveler idea because of his concern that "sleeper agents" of a terrorist organization could learn what factors qualified a person for entry into such a program and infiltrate a non-suspicious person into it, who might wait years before taking advantage of the less intense scrutiny to carry out a terrorist attack on an aircraft. This is a legitimate concern, but it is no different in principle from the concern over granting very high-level security clearances to people who will have access to nuclear weapons designs and other highly sensitive information. No such system of clearances can ever be perfect, but safeguards can be built into it to make this form of subversion unlikely to work for a terrorist organization.

One safeguard against "sleeper agents" is to periodically re-clear members of the Registered Traveler program, perhaps at random intervals. A person should not be cleared once and then considered qualified forever, regardless of future behavior, travel patterns, etc. And obviously, members of the program would still be checked against current watch lists by CAPPS-II every time they made reservations for a plane trip, just like all other travelers.

Another safeguard is to include an element of random selection into the baggage-screening process for Registered Travelers. Despite these passengers having been cleared in advance, a fraction of their bags should still be processed as if they belonged to selectees. As RAND's briefing on positive passenger profiling has suggested, this percentage could be varied, with a larger fraction of such bags going through high-level screening when excess capacity is available in the system. RAND calls this "adaptive profiling." It would introduce an important element of randomness into the processing of Registered Travelers that would reduce the odds of success of any attempted "sleeper agent" strategy.

2. Outsmarting the Selectee Process

The other concern is that terrorists could outwit a CAPPS-type approach for selecting out high-risk travelers for extra scrutiny. One expression of this perspective is the "Carnival Booth" simulation produced by a group of MIT graduate students.[32] The basic premise is that any attempt to use profiling (e.g., CAPPS) techniques to identify high-risk passengers for extra scrutiny can be defeated by a terrorist organization willing to probe the system enough times. As the authors put it, "the fact that individuals know their CAPS [sic] status enables the system to be reverse engineered." In other words, the terrorist cell sends members on probing missions, taking plane trips to see which of their members do *not* get flagged for extra scrutiny. Those who are repeatedly passed over can then be used, reasonably safely, to carry out actual terror missions. The "Carnival Booth Effect" comes about, the authors maintain, because the system entices terrorists to "Step right up and see if you're a winner." The paper develops equations and reports on a simulation modeling exercise attempting to demonstrate, quantitatively, that a CAPPS-type system will end up being less effective than a system based solely on randomized scrutiny.

Clearly, this critique depends on a number of key assumptions. Some of the most important are the following:

- That the profile used in a CAPPS-type system is static over a long period of time;
- That the terrorist group has enough people, organization, and patience to systematically probe the system;
- That selectees always know their status, i.e., that they have been singled out for extra scrutiny.

In addition, of course, since the MIT students do not know many details of how the current or future CAPPS operates, they had to make a number of other assumptions (e.g., about the range of distribution of scores for selectees and non-selectees).

Let's assume for the sake of argument that the Carnival Booth modelers have a point—i.e., that under the assumptions they make, a disciplined terrorist organization could undermine the effectiveness of a CAPPS-based system. How could a risk-based system be designed to minimize those effects?

The key theme for countering the Carnival Booth Effect is to reduce the predictability of the system. First, the algorithm used for selecting high-risk persons should not be static; though its broad outlines are not likely to change over time, it should be continually fine-tuned as additional information is learned about the characteristics and behavior of terrorists and their organizations. Thus, a cell member not flagged in September might well be flagged in November.

A second factor is to minimize the extent to which passengers know their selectee status. If boarding passes are marked only electronically (and not visually), those who are actually in the high-risk group may not realize that they have been so designated. While all selectees will pass through additional screening at the checkpoint, as described in Part 4, this additional screening should also be provided to a random subset of ordinary passengers, thereby making it much less obvious which of those going through the backscatter X-ray have actually been included in the high-risk group. It might only become obvious which of these passengers had been designated high-risk if that enhanced screening actually detected a prohibited object on that person's body, in which case the system would have done its job and the person would be subject to interrogation and possibly arrest. However, such objects might also be detected on the bodies of non-terrorists, so even being flagged by this screening would not equate to being identified as a possible terrorist.

There are also clear implications for the design and location of checked-baggage screening. Lobby installations, where bags are inspected in full view of passengers, can provide a clear tip-off to passengers that they have been designated as a selectee; they can see their bag being processed differently. All such explosive-detection inspections should occur within the normal baggage-processing facilities, out of the view of passengers. (This will also prevent a booby-trapped suitcase bomb from being exploded in the midst of a crowded ticket lobby.)

Part 6

Conclusions and Recommendations

America's current approach to airport security is seriously flawed. By devoting equal resources to every passenger and every piece of luggage, it spends too much on people who are no threat and too little on the few who might be. It therefore wastes scarce security resources and produces less security than would a better-targeted approach.

Moreover, the policy being applied to airport security is out of sync with most other security policies. In cargo shipment—by air, truck, and water—risk-based approaches are well-established and well-accepted. And in any number of cases involving the entry of both citizens and non-citizens into the nation, the federal government makes use of a number of risk-based approaches, especially those that pre-clear subsets of people based on their voluntarily signing up and providing detailed information about themselves.

The Transportation Security Administration, since Admiral Loy took over, seems to be moving toward a risk-based approach. It is working on two key elements needed for such a system: a means of pre-clearing low-risk air travelers (now called Registered Traveler) and a means of selecting out high-risk travelers (now called CAPPS-II). But these efforts need modification, both to better safeguard Americans' privacy and to take better advantage of their capabilities in the screening of passengers and baggage.

Both Registered Traveler and CAPPS-II seem to be heading in the direction of compiling and maintaining intrusive databases on air travelers, going far beyond what is needed in the case of the proposed CAPPS-II and risking adverse reaction from frequent fliers in the case of Registered Traveler. While the RT program does require the existence of an ongoing membership database, it should be maintained by one or more private data management firms, akin to Visa and MasterCard. They would interface with TSA for the actual clearance decisions and with the airlines for customer interactions.

The risk-screening function does not require the creation of a massive, privacy-invading database on all air travelers. The basic requirements of an improved CAPPS are (1) real-time cross-checking of all government watch lists, (2) full use of airline reservation system data on passengers, and (3) ongoing improvements in algorithms and weighting factors. Efforts by TSA to create an "Airline Echelon" that probes the personal and financial lives of all air travelers (such as its proposed Aviation Security Screening Records database) should be prohibited by Congress, as part of its oversight function.

Taking full advantage of the tools for sorting passengers into high-, low-, and medium-risk groups will mean changes in the processing of both checked baggage and passengers. A risk-based baggage processing system calls for using the most costly (and potentially slowest) explosive detection systems on all high-risk bags and a random fraction of other bags, with most bags inspected by faster, automated systems. All checked baggage inspection should be carried out in secure baggage areas, not in ticket lobbies filled with

passengers—both to protect passengers from the possibility of explosions and to reduce the extent to which selectees are aware that their bags are receiving special scrutiny.

A risk-based passenger screening system requires redesigned passenger checkpoints, providing expedited lines for Registered Travelers and adding post-screening facilities at which selectees (all high-risk passengers and a random fraction of medium-risk ones) can be screened by body-scanning systems. To put an end to gate screening, all passengers must obtain boarding passes prior to passing through the screening checkpoints. To prevent overly long lines at ticket counters, that will require more ticket lobby kiosks at which e-ticket holders can receive boarding passes. Special kiosks must also be provided for Registered Travelers.

To summarize our recommendations for a risk-based airport security system, Congress should do the following:

- Require the TSA to test and then implement a Registered Traveler program;
- Require that private sector service bureau(s) operate the Registered Traveler database(s), interfacing with the TSA and the airlines;
- Prohibit the TSA from implementing a CAPPS-II system that employs data-mining of databases on the personal and financial details of all airline passengers;
- Re-interpret the 100 percent checked baggage screening requirement of the Aviation & Transportation Security Act to permit the use of high-speed, automated X-ray systems for first-tier screening, consistent with their use for carry-on bag screening.

Airports should make the following changes, with the support and encouragement of the TSA:

- Configure all checked baggage screening "in-line," as part of the normal flow of baggage processing and away from ticket lobbies;
- Provide ample space in ticket lobbies for airline installation of two types of check-in kiosks, one type for Registered Travelers and the other type for all other passengers;
- Reconfigure passenger screening checkpoints to provide separate lanes for Registered Travelers;
- Provide additional secondary screening facilities at the checkpoints, to permit further searches of both the persons and hand baggage of selectee passengers.

Shifting to a risk-based approach will permit limited security resources to be better targeted in the airport segment of transportation. To fully implement Congress's original intent regarding 100 percent checked baggage screening via EDS would require a capital expenditure of some $12 billion, using RAND's estimate of the number of EDS machines required to do the job at an acceptable level of performance.[33] And the annual cost of staffing those machines would be around $2 billion. That is far too much to devote simply to checked airline luggage—which is, after all, but one piece of passenger airline security. The broader picture of transportation security also includes air cargo, general aviation, seaports, trucking, railroads, ferries, bridges and tunnels, etc.

The creation of a new Department of Homeland Security offers the opportunity to step back and take a more careful look at the cost-effectiveness of current aviation security efforts. It may well be that increased investment in intelligence and law enforcement would be significantly more cost-effective than the many billions now being devoted just to the commercial air passenger sector.

About the Authors

Robert W. Poole, Jr. is Director of Transportation Studies at Reason Foundation in Los Angeles. He received B.S. and M.S. degrees in engineering from MIT. He has advised the U.S., California, and Florida Departments of Transportation, as well as the White House Office of Policy Development and/or National Economic Council in the Reagan, Bush, Clinton, and Bush administrations. He was a member of Pres. George W. Bush's transition team.

George Passantino is Director of Public Affairs for Reason Foundation. In this role, George is responsible for Reason's efforts to convert cutting-edge policy ideas into workable, real-world policy change through direct interaction with public officials and staff, key stakeholder organizations, and allied groups.

Other Relevant RPPI Policy Studies

Re-thinking Checked-Baggage Screening. By Viggo Butler and Robert W. Poole, Jr., Policy Study No. 297, July 2002.

Improving Airport Passenger Screening. By Robert W. Poole, Jr., Policy Study No. 298, September 2002.

Appendix

Current U.S. Risk-based Programs in Transportation

A. INSPASS

The Immigration & Naturalization Service Passenger Accelerated Service System (INSPASS) is a kind of trusted traveler program for U.S. citizens returning from overseas. It was authorized as part of a 1990 law that mandated that immigration waiting periods be limited to 45 minutes. Under the program, citizens who wish to participate complete a half-hour registration process, providing background information which the INS can check, and must also permit their hand geometry to be recorded as a biometric identifier. Upon returning to the United States from overseas, an INSPASS member bypasses normal immigration lines and makes use of a special self-service kiosk. At the kiosk, the passenger responds to questions on the screen and places his/her palm on a scanner, obtaining clearance to enter in less than a minute, without having to wait in a long line.

While very popular with frequent international travelers, the program has been plagued by equipment problems, lack of marketing by the INS, and hassles involved in signing up (primarily, having to go to an INS office to submit the original handprint, rather than being able to do so at the airport). INSPASS is being phased out, but a replacement is promised by the INS within the next two years.[34]

B. APIS

Another current risk-based program is the Advance Passenger Information System (APIS). Initially a voluntary effort begun by airlines and the Customs Service in 1988, APIS calls for airlines that bring passengers from overseas to the United States to provide Customs, in advance, with the name, sex, passport number, and visa number or resident alien card number (if applicable) of each passenger and crew member prior to its departure for this country. Before the flight lands, the list is checked against records of about two dozen federal agencies, to enable high-risk passengers to be given extra scrutiny when they are processed upon landing. The Aviation & Transportation Security Act of 2001 made APIS mandatory for all airlines, the penalty being denial of U.S. landing rights.[35] During the interim period, before the law's Jan. 18, 2002 deadline for compliance, passengers on foreign airlines not participating were processed separately from others. In January 2003 the INS proposed additional data requirements, intended to separate "high-risk" from other passengers in using the system."[36]

C. NEXUS

In the aftermath of 9/11, the United States and Canada developed a border crossing "fast lane" program called NEXUS. Its purpose is "to speed the flow of pre-screened, low-risk travelers so we can focus our resources on higher-risk travelers."[37] The initial NEXUS lanes opened at the two main border crossings between British Columbia and Washington in June 2002, with similar lanes projected to be available by year-end at all major border crossings in Southern Ontario, New York, and Michigan—and at all other high-volume border crossings in 2003. The schedule for deployment was updated in December 2002.[38] A NEXUS-Air pilot project will be launched at Ottawa and Dorval International Airports in early 2003.

D. SENTRI

The U.S.-Mexico border has a similar program called SENTRI that pre-dates 9/11, having begun in 2000.[39] Aimed at frequent cross-border commuters, it reserves fast lanes for people who have enrolled by paying a fee and undergoing a criminal background check. Participating cars are equipped with a transponder, similar to those used for electronic toll collection. Once the car reaches a checkpoint (via the fast lane), a computer has retrieved the driver's photo and other identifying information, which permits quick approval for crossing. SENTRI has greatly reduced waiting time for its 12,000 participants. A local organization called San Diego Dialogue has called for a major expansion of the program. It argues that 312,000 frequent crossers account for 96 percent of entries at the San Ysidro and Otay Mesa crossings between Mexico and San Diego; thus, getting a larger fraction of them enrolled in SENTRI would reduce the otherwise very long lines at these crossing points.

E. PAL

In addition to SENTRI, the INS operates another frequent traveler program, this one for drivers on I-5 in California who traverse the Border Patrol's San Clemente Checkpoint.[40] Those who drive this route frequently and wish to avoid the occasional long back-ups at the checkpoint can apply for entry into the Pre-enrolled Access Lane (PAL) program, permitting them to use an express lane instead of the regular traffic lanes. Participants must enroll in person, with their vehicle, providing various identification documents and agreeing to submit to fingerprinting and an FBI check. Approved drivers' vehicles are equipped with a bar code decal, granting access to the PAL Lane.

F. Known Shipper

In both air cargo and surface cargo operations, the federal government is placing considerable reliance on "known shipper" programs as a principal tool for improved security. The basic principle is that instead of requiring every piece of cargo on every plane, truck, or ship to be inspected (as is now mandated for airline passengers' checked baggage), cargo containers are presumed to be safe and not needing to be inspected if they are put into the system by a shipper who is known to be low-risk. Continental Airlines began such a program in the late 1990s, developing software to identify the origins of all cargo before it is loaded onto planes. Shortly after 9/11, the Federal Aviation Administration fleshed out known shipper rules, and Congress adopted the idea in the Aviation & Transportation Security Act. By November 2002, shipments not

tendered by known shippers must be screened by an explosive detection system in order to be carried by air.[41]

For surface freight, the Customs Service is also implementing a known shipper program. Its initial pilot program, for the U.S-Canadian border, was unveiled in April 2002.[42] Sixty leading companies are taking part. Their trucks are equipped with transponders so that they can be passed through checkpoints without stopping, subject to occasional random spot-checks. To be approved for the program, companies must upgrade their own security, doing employee background checks, controlling access to their loading docks, and undergoing a security review by Customs. As *The Wall Street Journal*'s article noted, Customs' objective is "to allow inspectors to focus more on cargo they consider high-risk."

Endnotes

1 Associated Press, “U.S. Lawmakers: Air Passenger Profile System Needs Revision,”, Feb. 27, 2002.

2 Michael Mecham, “Flying Less, Irritated More—Biz Travelers Sound Off,” *Aviation Week & Space Technology*, April 29, 2002, p. 64.

3 Barbara De Lollis, “ ‘Trusted-Traveler’ Card Could Speed Security Check,” *USA Today*, July 1, 2002.

4 “State of the Airline Industry One Year After 9/11,” Washington, D.C.: Air Transport Association, September 2002, p. 13.

5 Viggo Butler and Robert W. Poole, Jr., *Rethinking Checked-Baggage Screening*, Policy Study No. 297 (Los Angeles: Reason Foundation, July 2002)and Gary Kauvar, Bernard Rostker, Russell Shaver, *Safer Skies: Baggage Screening and Beyond*, Santa Monica, CA: RAND National Security Research Division, 2002.

6 Gavin de Becker, *Fear Less: Real Truth About Risk, Safety, and Security in a Time of Terrorism* (New York: Little, Brown and Company, 2002).

7 John Croft, “Israeli Security Experts: Technology Not the Answer,” *Aviation Week & Space Technology*, November 26, 2001.

8 Personal communication to Robert Poole from Henk Guitjens, Schiphol Group, Oct. 3, 2002.

9 Information is available at www.schiphol.nl/schiphol/privium/privium_home.jsp.

10 Kevin J. Delaney and Paulo Prada, “IBM to Unveil Biometric Pact,” *The Wall Street Journal*, April 25, 2002.

11 Prague News Agency, “Passenger Smart-Card Trial to Launch at Two Airports in Europe,” *Airports*, May 7, 2002.

12 David Crawfords and Daniel Michaels, "Europe Is Scrambling to Meet Airline Security Commitments," *Wall Street Journal*, March 27, 2003.

13 David Armstrong and Joseph Pereira, “Nation’s Airlines Adopt Aggressive Measures for Passenger Profiling,” *The Wall Street Journal*, October 23, 2001.

14 Personal communications to Robert Poole from airline industry official, Oct. 11 and 15, 2002.

15 Personal communication to Robert Poole from airline industry official, Oct. 11, 2002.

16 Personal communication to Robert Poole from airline security official, Nov. 27, 2002.

17 Matthew Wald, “Plan Sharply Tightens Airport Screening,” *New York Times*, May 30, 2002.

18 Federal Register, Vol. 68, No. 10, January 15, 2003, pages 2102-2103.

19 Ann Davis, Joseph Pereira, and William M. Bulkeley, “Security Concerns Bring Focus on Translating Body Language,” *The Wall Street Journal*, August 15, 2002.

20 “Snapshots,” *Airports*, November 19, 2002, p. 4.

21 General Accounting Office, “Aviation Security: Registered Traveler Program Policy and Implementation Issues,” Washington, D.C.: GAO-03-253, November 2002.

[22] Gary Kauvar, Bernard Rostker, Russell Shaver, "Safer Skies: Baggage Screening and Beyond," Santa Monica, CA: RAND National Security Research Division, 2002.

[23] Michael E. Levine and Richard Golaszewski, "E-Z Pass for Aviation," *Airport Magazine*, November/December 2001.

[24] "'Smart Security': Proposal for a Pilot Demonstration For a 'Registered Traveler/Employee' Security Pilot Program," Washington, D.C.: Air Transport Association, August 19, 2002.

[25] Gary Kauvar, Bernard Rostker, Russell Shaver, "Safer Skies: Baggage Screening and Beyond," Santa Monica, CA: RAND National Security Research Division, 2002.

[26] Russell Shaver, "Quantifying the Case for Positive Passenger Profiling," RAND Powerpoint briefing, July 10, 2002.

[27] Barry Steinhardt, "Loss of Privacy Is a Cost," *USA Today*, January 28, 2002.

[28] Gregory T. Nojeim, "Civil Liberties Implications of Airport Security Measures," statement before the White House Commission on Aviation Safety and Security, September 5, 1996.

[29] Robert A. Levy, "Security and Freedom in a Free Society," *Cato Policy Report*, September/October 2002.

[30] Clyde Wayne Crews, Jr., "The Pentagon's Total Information Awareness Project: Americans Under the Microscope?" Cato TechKnowledge, Nov. 26, 2002; and Jeffrey Rosen, "Security Check: How to Stop Big Brother," *The New Republic*, Dec. 16, 2002.

[31] This term comes from airline information technology consultant Robert W. Mann, private correspondence, November 19, 2002.

[32] Samidh Chakrabarti and Aaron Strauss, "Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System," May 16, 2002.

[33] Viggo Butler and Robert W. Poole, Jr., "Rethinking Checked-Baggage Screening," Policy Study No. 297 (Los Angeles: Reason Foundation, July 2002), pp. 6-7.

[34] Jane Costello, "As Government Studies Biometrics, One Program Offers Cautionary Tale," *The Wall Street Journal Online*, Feb. 21, 2002.

[35] Jonathan Peterson, "Foreign Airlines Face New U.S. Scrutiny," *Los Angeles Times*, Nov. 30, 2001.

[36] Frances Fiorino, "Changes in INS Manifest Rules Target 'High-Risk' Passengers," *Aviation Week & Space Technology*, January 13, 2003.

[37] Joint statement by Deputy Prime Minister John Manley and Homeland Security Director Tom Ridge, June 26, 2002.

[38] "U.S., Canada Update 30-Point Agreement on Border Crossings," *Homeland Security & Defense*, December 11, 2002.

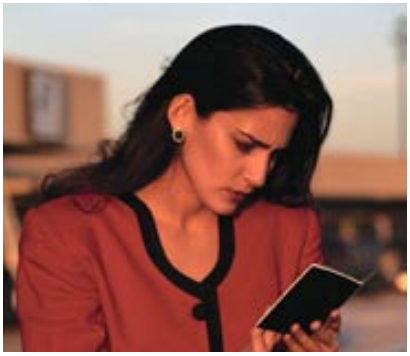
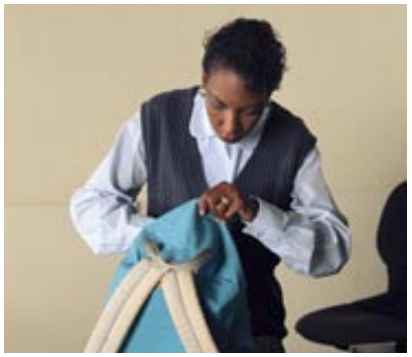
[39] Ken Ellingwood, "Easing the Bottleneck at the Border," *Los Angeles Times*, Dec. 14, 2001.

[40] "Pre-enrolled Access Lane Enrollment (PAL)," www.ins.gov.

[41] Kristin S. Krause, "More Air Cargo Security," *Traffic World*, Dec. 3, 2001 and "Magaw Talks Cargo," *Traffic World*, June 3, 2002.

[42] Gary Fields, "Customs Unveils Security Moves," *The Wall Street Journal*, April 16, 2002.





Reason Public Policy Institute
3415 S. Sepulveda Blvd., Suite 400
Los Angeles, CA 90034
310/391-2245
310/391-4395 (fax)
www.rppi.org

A RISK-BASED AIRPORT SECURITY POLICY - Reason Foundation. READ. Show more documents.Â May 2003 A RISK-BASED AIRPORT SECURITY POLICYBy Robert W. Poole, Jr. with George PassantinoProject Director: Robert W. Poole, Jr.POLICYSTUDY308. Page 2 and 3: Reason Public Policy Institutedivis. Risk-Based Airport Security Models. March 1, 2010 - 22:12 â€" wbeadling. Todayâ€™s U.S. airport security policy rests on a fallacious proposition. By applying equal screening resources to all passengers and all bags, the system acts as if security officials believe that every passenger and every bag is equally likely to be a threat. This premise wastes limited security resources on low-risk passengers and bags, thereby devoting less resources to higher-risk passengers and bags. In addition, this approach has created a â€œhassle factorâ€ at airports that drives away airline passengers. Credible estima 6. a) What is â€œrisk based securityâ€? b) Shmuel Zakay doesnâ€™t think Israelâ€™s security procedures would work in much larger European countries. Although they have five times as many passengers, these countries also have much greater resources. Do you think Europe should implement Israeli type security?Â Security operates on several levels: All cars, taxis, buses and trucks go through a preliminary security checkpoint before entering the airport compound. Armed guards spot-check the vehicles by looking into cars, taxis and boarding buses, exchanging a few words with the driver and passengers. Armed security personnel stationed at the terminal entrances keep a close watch on those who enter the buildings.