S. HRG. 108–990

OVERSIGHT ON TRANSPORTATION SECURITY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 9, 2003

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

91–310 PDF WASHINGTON : 2014

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina, *Ranking*
CONRAD BURNS, Montana	DANIEL K. INOUYE, Hawaii
TRENT LOTT, Mississippi	JOHN D. ROCKEFELLER IV, West Virginia
KAY BAILEY HUTCHISON, Texas	JOHN F. KERRY, Massachusetts
OLYMPIA J. SNOWE, Maine	JOHN B. BREAUX, Louisiana
SAM BROWNBACK, Kansas	BYRON L. DORGAN, North Dakota
GORDON H. SMITH, Oregon	RON WYDEN, Oregon
PETER G. FITZGERALD, Illinois	BARBARA BOXER, California
JOHN ENSIGN, Nevada	BILL NELSON, Florida
GEORGE ALLEN, Virginia	MARIA CANTWELL, Washington
JOHN E. SUNUNU, New Hampshire	FRANK R. LAUTENBERG, New Jersey

JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ROBERT W. CHAMBERLIN, *Republican Chief Counsel*
KEVIN D. KAYES, *Democratic Staff Director and Chief Counsel*
GREGG ELIAS, *Democratic General Counsel*

CONTENTS

WITNESSES

APPENDIX

OVERSIGHT ON TRANSPORTATION SECURITY

TUESDAY, SEPTEMBER 9, 2003

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 9:30 a.m. in room SR–253, Russell Senate Office Building, Hon. John McCain, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

The CHAIRMAN. Good morning. As we approach the second anniversary of the terrorist attacks on the United States, it's appropriate that we again focus our attention on transportation security. Since that fateful day, our Nation has been fighting the war on terrorism, whether it's our security abroad or at home. We can't afford to lapse into complacency as we grow accustomed to the so-called new kind of normal. Much has been accomplished over the last 2 years, and I think many would agree that transportation security is at its highest level ever, particularly aviation security. However, we need to remain vigilant across all modes of transportation, for the threat to our country has not waned. If we're serious about countering terrorist threats, and we are, we need to have confidence in our security efforts across all modes of transportation, and that requires our continued attention to instituting or upgrading sound and reasoned security initiatives.

Today's hearing is intended to provide both a forum foro know is, reviewing what has occurred over the last 2 years and to determine what remains to be done to strengthen transportation security, and how we can do it. With respect to aviation security, we must ensure that the accomplishments of the Transportation Security Administration are not lost.

Over the last 6 months, the TSA has reduced its screener workforce by 6,000 due to budgetary and appropriations pressures. While there has been a lot of discussion in the press about the impact of these reductions on waiting times at checkpoints, the real question we need to know is, what is the impact on security? A screener corps that is overworked and stretched too thin is simply not going to be able to carry out the job we're relying on them to do.

With respect to ground transportation, we need to make sure that the independent actions initiated so far by TSA, the DOT, and industry are followed up with a systematic program of security enhancements based on each mode's particular needs. Clearly, there's

need to enhance security on our highway and transit networks, yet both are intentionally open and easily accessible and, therefore, more difficult to harden against terrorist attacks. Railroads and pipelines, for their extensive unprotected rights of way, also present unique challenges.

Further, we need to make sure that safety and security efforts at DOT and the Department of Homeland Security are adequately coordinated, since safety and security so often overlap.

Maritime security, because of the immense volume of trade that must move through our Nation's ports, remains a daunting task. While the Administration has taken action to implement the many important requirements of the Maritime Security Act of 2002, many in the maritime community still wonder who is in charge. They're confused by what, in some cases, appears to be competing requirements of the various agencies claiming responsibility for maritime security. Such confusion, not unique to the maritime industry, is compounded by the lack of agreements between the various agencies and departments responsible for transportation security. Transportation security is far too important to be placed in limbo due to needless agency turf battles. I hope our witnesses today can finally clarify the roles and relationships of the agencies they represent.

Our country was the victim of a terrible crime. Its after-effects will continue to be felt. We must be diligent in protecting our country, but always be cognizant of the burdens we're placing on our citizens and industries.

I thank our witnesses for being here and welcome their insights into transportation security.

Senator Hollings?

STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Senator HOLLINGS. Thank you very much, Mr. Chairman, for the hearing.

I'll ask that my prepared statement be included.

The CHAIRMAN. Without objection.

[The prepared statement of Senator Hollings follows:]

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

September 11 changed our world forever. It has changed our travel patterns, it has changed the way we balance civil liberties against security requirements, and ultimately it has changed the focus of our government. Terrorism is a war, and it is a war that is perpetrated against innocent civilians, so the stakes are extremely high, and failure could have catastrophic effects, not only on the lives of innocent civilians, but also on the economic health arid welfare of our nation. Sunday night the President announced the Administration wants an additional $87 billion to fight terrorism in Iraq, bringing the total amount spent in Iraq to $150 billion. This amount represents close to 5 times the amount of money that the President proposed to spend on our homeland security this year. We must be able to fight this war on two fronts—in Iraq and at home.

I personally was reluctant to create a Department of Homeland Security to address the issues confronting us because of the horrific terrorists attacks. In fact, I was concerned that bureaucratic reshuffling, without prior planning, would detract from our ability to prepare and respond to threats of terrorism. However, we are stuck with what we have, and the Administration must take the steps necessary to help this bureaucracy work. Underfunding key transportation security initiatives,

and I know you all have to deal with OMB and the White House for your budgets, is not a choice we can afford. I still am very concerned that your agencies have a long way to go before you can claim coordinated integration and that petty bureaucracies have been overcome, and while we have some good people working on the problems, I think that the Administration has not dedicated the necessary resources to help you do the job. For example, we are busy taking pictures of the President in front of the Coast Guard at the vitally important Port of Philadelphia, yet we are not providing the port security funds for Philadelphia to comply with its federally approved security plan. In fact we are not even providing funding for the Coast Guard to review the security plan. This year, the President's budget had not one penny explicitly provided to help ports comply with the Federal mandates for port security. When we passed the Maritime Transportation Security Act, the Senate insisted on a user fee. Unfortunately in order to gain passage of the bill we relented and we passed the bill without a user fee because I was convinced by some that this was important and would be supported by the Administration. Well the Administration was too busy focusing on the tax cut to provide more than meaningful glance at port security, and I have not been able to get votes needed to ensure this funding.

However, that is water under the bridge, and we need to move forward and make sure that we provide the citizens of the United States a secure transportation system. We saw after 9/11 that without an enhanced security system, people would not get back onto planes. We had to bail out the airline industry twice and invest billions. People all over the United States are concerned about the issue of transportation security. but as a nation we should be able to provide them the security they deserve, and they should not have to be concerned about getting on an airplane or riding Amtrak or traveling through the Holland Tunnel from New Jersey into Manhattan.

Our witnesses sit here today having done a remarkable job with what they have been provided. For instance, over the past year and a half, almost all of reports suggest that under the guidance of Admiral Loy, aviation security has improved dramatically that the screening workforce is well trained and doing a good job. But, and this is where we have problems—funding remains critical. You can not take the aggressive steps needed for cargo security, for research on new explosive detection systems, and for training of Federal Air Marshals without the money. You can not run an agency when Congress is putting in artificial staffing caps, forcing you to "right size" the screener workforce that will result in longer lines at the airports. That makes no sense. I know you have to do what you are told and we both understand that.

We have a long way to go at our seaports. Although the Coast Guard has stepped up to its new responsibilities for homeland security with its usual vigor and "can do" attitude, I have some very serious concerns that you are not able to implement the new Maritime Security Transportation Act to secure our ports. For instance, the Act mandated that certain large commercial vessels carry transponders to allow us to monitor their movements, to help ensure that an oil tanker was not hijacked and run into one of the many nuclear reactors located on our navigable waterways, yet the President's budget included only $1 million to actually purchase the towers and equipment necessary to start monitoring the cruise ships and oil tankers that already are carrying identification equipment, and because of the insistence of the OMB, they proposed delaying this project until 2007. This is not right. While I am pleased that the Coast Guard receives an increase in your budget, I would say that this increase is long overdue, and yet it is still unclear if this increase is enough to ensure that all of the Coast Guard's security and non-security missions are adequately funded.

In general, I have real concerns about the whole surface transportation security issue as well. We need to do more in this area. The rail system traverses the entire nation, and our passenger rail service operates through and under many of the most important structures in the nation. We need to have a plan, and we need to follow through with the necessary resources to secure this system, as well as our other surface modes which move 800,000 shipments of hazardous materials annually.

None of us want to shortchange transportation security. The Administration has got to let you do your job and provide the resources necessary to build a security system, like the one the Israeli's used—the onion, with layers and layers of protections. I look forward to the statements of the witnesses.

Senator HOLLINGS. And I was a little tardy because I was trying to figure out the exact figures. And I want the witnesses to correct what I have here, from the best staff in the U.S. Senate.

[Laughter.]

Senator HOLLINGS. Airports. These are the figures, for, that we need, according to our figures and everything else of that kind. GAO, for example—and we've got the report in front of us—is $5 billion more. We need to get the equipment for the baggage check and the additional redesign and everything else like that, a $5 billion amount. Tell me why that's right or wrong.

Ports, seven and a half billion. We told all the ports, Mr. Chairman, to prepare plans and everything else. Now they've submitted them, and everything else of that kind, and to flesh out those ports plans, seven and a half billion dollars. The Coast Guard needs an additional $500-million-point-five. Admiral Collins, tell me if we need more. I know at one time, the overall was about $7 billion for the Coast Guard. We've been putting some in there. I want to make sure the AIS towers are covered in the extra cost, and even craft, if we need them. That was a low figure. I was trying to get it up higher, and that's why I was late. Rail security, $3 billion, for Amtrak and for the tunnels and what have you. The highways and transit, the states say $2 billion is needed there. And Mr. Bonner, Customs, I understand for cargo security the need is about $2 billion.

So overall, you add up the airports, the ports, the Coast Guard, the rail security, the highways and transit, the Customs and cargo security, $20 billion. Now, we've got $87 billion for Iraq, Senator Lautenberg. I'm more for $87 billion for the United States this morning.

Getting right to the point, getting $87 billion for the U.S., let me tell you how that works, Mr. Chairman. They expect that to be cut back, probably, to $77 billion. You know how we've got to try to act like we've really reviewed it in detail and done our jobs, so we'll cut that back to $77 billion. The $20 billion for the transportation needs here will cut us back to some $50 billion, and we'll hold that $20 billion until next year's campaign and then Karl Rove will dish it out. So whatever we can get, don't expect to get it here this year, and don't expect to get it before March or April of next year, but, in the campaign, $20 billion will go around all over the durn countryside.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you for that optimistic overview——

[Laughter.]

The CHAIRMAN.—Senator Hollings.

Senator Lott?

STATEMENT OF HON. TRENT LOTT,
U.S. SENATOR FROM MISSISSIPPI

Senator LOTT. Thank you, Mr. Chairman, for having this hearing.

Certainly, it's appropriate, as we mark the two-year anniversary of 9/11/2001, we need to take a look at our transportation security. And you have undertaken a daunting and awesome task, and I think you should be commended, all of you here at the table, for the work that you've done and for the effort that's still underway. Obviously, we've not done everything we need to do, and we haven't always done it to perfection. But Congress mandated a real

challenge for you after the events of 9/11. We basically told you to completely overhaul security and aviation, and you went after it, and you got it done. And now, sometimes when you do things in haste or under mandate from Congress, you don't get it all right, so we need to take a look at where we are and what additional funds you need or what additional authority you might need or what we need to do to change that.

In the FAA Federal Aviation Reauthorization Conference Report, we did try to do a number of things that would help TSA with its burdens. We need to continue to do more. We've had, obviously, some things, some responsibility for the costs assigned in the wrong place. We'd like to get that more fairly and equitably assigned in the industry and with the government. I am concerned about AIP funds that have been diverted from the airport improvements over into the security area on a temporary basis. That was something we had to do, but I hope that certainly we don't plan on continuing that.

Under the persistence of Senator Hutchison, of course, we've had the cargo security bill passed. We need to continue to look very seriously at port and maritime security. Being from a state that's got a river along one side and the Gulf of Mexico on the other, and the ports of Pascagoula, Gulf Port, Bienville, and even New Orleans right in the area, I continue to worry about how secure they are. Coast Guard has an important role in that area, and we're working to add additional cutters, aircraft, command and control, and, of course, the Deepwater program, but I think we need to continue to ask ourselves just how secure we are.

So I'll look forward to your testimony, and I'll have some questions based on my statement.

Thank you, Senator McCain.

The CHAIRMAN. Senator Lautenberg?

STATEMENT OF HON. FRANK R. LAUTENBERG,
U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Thank you, Mr. Chairman.

And I welcome all the witnesses here, who have a significant task. Some of it is to—that task is to prove to Congress that we can get done what we'd like to get done with less and less funding to do it than is anticipated.

This hearing, on the eve of the second anniversary of 9/11, is a very important one, and I wish I could tell my constituents, many of whom lost loved ones that terrible day nearly 2 years ago, that they're much safer now than they were then. But I can't say it with certainty. I'm not sure that what we've offered thus far has done the job.

There was a disconcerting article in Sunday's *Washington Post,* entitled "Government's Hobbled Giant," that talked about the slow start, confusion, and low morale at the Department of Homeland Security. The President initially resisted creating DHS, and I have to wonder if he's fully committed to giving the Department the resources it needs to do the job that it must do, especially with regard to securing our transportation network.

Inexplicably, the Administration moved to cut the number of airport baggage screeners and law enforcement officers, at a time

when the threat level was being raised. Inexplicably, the Administration proposed to cut funding for the Federal Air Marshal Program, just one day after citing specific terrorist threats to commercial air travel. Inexplicably, the Administration still fails to adequately fund port security, which remains highly vulnerable. Terrorists have tried to smuggle all sorts of weapons and even themselves inside shipping containers, and only a fraction of which are getting inspected. Inexplicably, the Administration remains obsessed with contracting out safety and security functions of the government, like air traffic control, with seeming disregard for the consequences it will have on our safety. And, all the while, the President stirs the hornet's nest by saying things like, "Bring them on."

Since the last time we held a hearing on transportation security, there have been a number of breaches, some of which have taken place in or near New Jersey. For example, an arms dealer was caught trying to smuggle a shoulder-fired surface-to-air missile into our ports for terrorists to use on our own soil. Now, that investigation—and thank goodness it was successful—this man was importing shoulder weapons, shoulder-launched weapons, from St. Petersburg to Baltimore, just like you might ship—who knows what?—caviar or something like that. And he had studied it well and thoroughly enough that he knew that that was a route that could probably succeed. I don't know whether we have 18 months to uncover some of these plots against us.

In another instance, three young men floated in a raft across Jamaica Bay and wandered onto the runway at JFK Airport and almost had to knock on the door of the police headquarters to be discovered. This happened just shortly after the Transportation Security Administration cut the number of law enforcement officers working at airports, went down from 64 to 19 at the three major airports in the New York/New Jersey region. It's time to disavow security on the cheap.

On Sunday night, the President finally, Senator Hollings, talked about a preliminary cost for the War in Iraq. You wouldn't bet the family farm that that's going to be the final number, I'll bet. And now we need to know what kind of costs it's going to take to keep Americans safe here at home.

While we have some improvements—and I congratulate those of you who have worked so diligently to try and organize this huge task force and to get the people in place—in the right places at the right time. So we've made some improvements with regard to transportation border security. And I'm sure that our witnesses will tell us about what we have to do to get where we'd like to finally be.

I thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

I want to welcome the witnesses again, and I thank you for appearing today.

And we'd begin with you, Mr. Shane. Thank you very much for being here.

STATEMENT OF JEFFREY N. SHANE, UNDER SECRETARY FOR POLICY, U.S. DEPARTMENT OF TRANSPORTATION

Mr. SHANE. Thanks very much, Mr. Chairman, Members of the Committee. We appreciate very much the Committee's decision to hold this important hearing on a very important issue.

In the two years since that most monstrous crime ever perpetrated on America was committed, we've made enormous strides in the transportation security area. Secretary Mineta said, earlier this year, that creating the Transportation Security Administration was by far the toughest, most challenging, and most satisfying endeavor he had ever undertaken. We all owe a great deal of thanks to Secretary Mineta, to our former Deputy Secretary Michael Jackson, and certainly to my good friend, Jim Loy, now the Transportation Security Administrator, for their unwavering commitment to this country and the superb work they did in creating TSA. Because of their efforts and those of thousands of others, the Department met every congressional deadline on time and, in the process, transformed the security of our aviation system within the span of just a few short months.

Mr. Chairman, I have a longer prepared statement. What I'd like to do, in the interest of time, is compress that and ask that the full statement be put into the record.

The CHAIRMAN. All prepared statements will be made part of the record, and thank you.

Mr. SHANE. Thank you very much.

While much of the focus since September 11 has been on aviation security, the Department has also been doing a great deal of work with our DHS counterparts in assessing the vulnerabilities and improving the security of our other modes of transportation. For example, the Maritime Administration has worked closely with the United States Coast Guard and TSA to evaluate security at our Nation's ports and to disseminate two rounds of port security grants facilitating $262 million in security upgrades. The Federal Transit Administration has also shared its expertise by funding $30 million in vulnerability assessments and the security training of transit operators across the country. Additionally, our Research and Special Programs Administration has worked closely with TSA to ensure that the transportation of hazardous materials fulfills both safety and security requirements. Finally, I've served, personally, as a Co-Chairman, together with Doug Browning, the Deputy Commissioner of Customs, a Co-Chairman of the Executive Steering Committee that oversees the Operation Safe Commerce Program. $58 million in Operation Safe Commerce grants was recently awarded to the three participating load-center ports. That's Los Angeles/Long Beach, Seattle/Tacoma, and New York/New Jersey. Through those grants, we are creating an essential test bed for new technologies designed to provide greater security for freight containers as they move on inter-modal journals through global commerce.

Since last March, of course, the primary responsibility for maintaining transportation security has been vested in the Department of Homeland Security. Two key elements of the DHS structure, DHS and the Coast Guard, came out of the Department of Transportation, and they remain key players, of course, in providing for

the Nation's transportation security. The close ties that we have, at DOT, to TSA and the Coast Guard have helped us to establish extremely close links throughout DHS, and we continue to working closely with our former colleagues, supporting them in every step of the way as they defend our Nation's homeland.

We have taken a great many steps to ensure that this close working relationship continues into the future, as well. For example, just prior to the creation of DHS, our Federal Aviation Administration and TSA signed a memorandum of agreement specifying in detail the specific role that each agency would play in overseeing the safety and security of our aviation system. We have signed memoranda of agreement in some other areas, as well, and we will continue to evaluate the need for additional agreements as we gain more experience. In addition, we have supplemented these formal MOAs with regular discussions at various levels between DOT and DHS on the full range of transportation security issues.

Finally, a key step we have taken is to designate a single point of contact for DHS and other agencies to access information about the transportation system, to tap into the network of contacts we have with our transportation stakeholders at DOT, and to learn from our technical expertise in dealing with complex issues, like the transport of hazardous materials. Our Office of Intelligence and Security has been designated as this formal point of contact and has played a key role in helping DOT support DHS on a number of critical issues in recent months.

Mr. Chairman, recent GAO reports have documented that significant challenges remain in transportation security, and suggest that more coordination between TSA and DOT is needed. The Department's Office of Intelligence and Security is providing that coordination while also representing DOT on over 40 security policy working groups.

The key asset that DOT brings to the security table is our involvement in the operation of transportation systems. The blackout that occurred last month provided a good example of the Department of Transportation's unique ability to assess the state of the transportation sector in multiple cities and in a very short time. We did it through our real-time communications network, with state, local and industry stakeholders. This information proved critical to DHS and other Federal decisionmakers throughout the incident.

Remember that our modal administrations have decades of experience in responding to all kinds of emergencies—floods, hurricanes, blizzards, hazardous materials spills, and, yes, blackouts. This operational expertise will remain an essential ingredient in our Nation's emergency response capability.

Thank you very much for the opportunity to appear here, and I certainly look forward to answering your questions at the appropriate time.

[The prepared statement of Mr. Shane follows:]

PREPARED STATEMENT OF JEFFREY N. SHANE, UNDER SECRETARY FOR POLICY, U.S. DEPARTMENT OF TRANSPORTATION

It is a pleasure to be here today to discuss transportation security issues. For nearly two years, since that awful day when Secretary Mineta was compelled to

ground all aircraft over the United States for the first time in history, the U.S. Department of Transportation has been working with the Department of Homeland Security to make our transportation system more secure. We applaud the Committee for holding this hearing, and look forward to continuing to work with you on these critical issues. The monstrous crime perpetrated on America on September 11 crystallized for all of us the importance of enhancing security across our transportation system, and while we have accomplished a great deal since that day, much more can be done.

As we discuss transportation security issues, it is also important, of course, to consider the substantial contribution that the transportation sector makes to our Nation's economy. For example, transportation-related industries currently account for approximately 11 percent of the Nation's GDP and 8 percent of our workforce. Transportation infrastructure and services enable our citizens to get to work or school, visit family, take vacations, and manage their businesses by moving materials, supplies, and products around the world as efficiently as possible, whether domestically or internationally. For all of these reasons, the importance of transportation to America's economic and social well-being cannot be overstated, and that is why maintaining the highest levels of security throughout the system is so critical to our prosperity as a Nation.

Past Accomplishments

Secretary Mineta said earlier this year, when the Transportation Security Administration (TSA) and U.S. Coast Guard were transferred to the new Department of Homeland Security, that creating TSA was by far the toughest, most challenging, and most satisfying endeavor he had ever undertaken. "Starting from a blank sheet of paper on November 19, 2001," Secretary Mineta said, "we created an agency of more than 60,000 employees that is truly fulfilling its goal of protecting Americans as they travel across our country, and beyond." We all owe a great deal to Secretary Mineta, to former Deputy Secretary Michael Jackson, and certainly to my good friend TSA Administrator Admiral Jim Loy for their unwavering commitment to this country and the superb work they did in creating TSA. Because of their efforts and those of thousands of others, the Department met every congressional deadline on time, and in the process transformed the security of our aviation system within the span of just a few short months.

While much of the focus since September 11 has been on aviation security, and rightfully so, the Department has also been doing a great deal of work with our DHS counterparts in assessing the vulnerabilities and improving the security in our other modes of transportation. For example, the Maritime Administration has worked closely with the Coast Guard and TSA to evaluate security at our Nation's ports and to disseminate two rounds of port security grants, facilitating $262 million in security upgrades as a result. The Federal Transit Administration has also shared its expertise by conducting $30 million in vulnerability assessments and security training of transit operators across the country. Additionally, the Research and Special Programs Administration has worked closely with TSA to ensure that the transportation of hazardous materials fulfills both safety and security requirements.

Finally, I have served personally as a co-chairman of the Executive Steering Committee that oversees the Operation Safe Commerce program. Fifty-eight million dollars in Operation Safe Commerce grants have recently been awarded to the three participating load center ports—Los Angeles/Long Beach, Seattle/Tacoma, and New York/New Jersey. Through these grants we are creating an essential test bed for new technologies designed to provide greater security for freight containers as they move on intermodal journeys through global commerce. Working closely with other federal agencies, these efforts across all other modes of transportation are designed to create a comprehensive system of measures that will provide far greater security across the entire international supply chain than anything we have known before.

Transition to DHS

Today, of course, the primary responsibility for maintaining transportation security lies with the Department of Homeland Security. Formed in March of this year, this new Department has allowed formerly diverse security functions spread across the government to come together in a unified structure. Two key pieces of the DHS structure—TSA and the Coast Guard—moved from the Department of Transportation to DHS and continue to play major roles in providing for the Nation's transportation security. The close ties that we have to these two agencies have helped us to establish extremely close links throughout DHS, and we continue working closely with our former colleagues, supporting them every step of the way as they defend our Nation's homeland.

We have taken numerous actions to ensure that this close working relationship continues into the future as well. For example, just prior to the creation of DHS, the Federal Aviation Administration and TSA signed a memorandum of agreement specifying in detail the specific role that each agency would play in overseeing the safety and security of our aviation system. Aviation poses unique challenges, of course, not only because it was used to carry out the September 11 attacks, but also because of the FAA's continuing responsibilities for managing the air traffic control system, and thus helping to secure our airways in times of crisis. Because of these considerations, we believed that it was very important to have a written agreement between DOT and DHS outlining exactly what each Department would be responsible for once TSA moved to the new department, and what we could expect from one another.

We have signed memoranda of agreement in some other areas as well, and will continue to evaluate the need for additional agreements as the need arises. Now that DHS is fully established we will be in a better position to determine what role each of our departments will play in providing security for the other modes of transportation. In addition, we have supplemented these formal MOAs with regular discussions, at various levels, between DOT and DHS on the full range of transportation security issues. One of the things we have done during this transition period to help manage our relationship is a regular meeting that I conduct with senior TSA staff on a bi-weekly basis. These meetings give us the opportunity to coordinate our activities, identify potential issues or problem areas, and ensure that we are providing all the support we can to help TSA in securing our Nation's transportation system.

Finally, another step we have taken is to designate a single point of contact for DHS and other agencies to access information about the transportation system, tap into the network of contacts we have with our stakeholders, or learn from our technical expertise in dealing with complex issues like the transport of hazardous materials. Our Office of Intelligence and Security has been designated as this formal point of contact and has played a key role in helping DOT support DHS on a number of critical issues in recent months. A good example of the benefit of this single point of contact was our experience with the recent suspension of the Transit Without Visa (TWOV) program in response to credible intelligence that terrorists intended to take advantage of this program to carry out additional attacks on the United States. DOT's Office of Intelligence and Security ensured that DHS had the information it needed to determine what the impact of that shutdown would be and helped it deal with the airline industry to ensure a smooth shutdown of the program.

Future Challenges and DOT's Role in Security

While some assume that security simply moved to DHS when TSA and the Coast Guard departed earlier this year, there is no question that DOT can continue to make important contributions to the development and implementation of transportation security policy. Recent GAO reports have documented that significant challenges remain in transportation security, and suggest that more coordination between TSA and DOT is needed. The Department's Office of Intelligence and Security provides that coordination service to the Secretary, while also representing the Department on over forty security policy working groups.

The Department of Transportation's mission is to ensure safety, mobility and the economic viability of the transportation system. Security is a fundamental element of each of these three key mission areas. To effectively integrate security into transportation decision-making, five enduring functions remain within DOT. They are: security policy development; transportation system design; intelligence; operations; and readiness, including plans and exercises.

One other important role that the Department can play is in regards to the operation of transportation systems. The blackout that occurred last month proved a good example of the Department of Transportation's unique ability to quickly assess the state of the transportation sector in multiple cities. This was done through our real-time communications network with state, local and industry stakeholders. This information proved crucial to DHS and other federal decision-makers as the crisis rapidly unfolded.

Finally, there is one additional reason why DOT must be at the table during security emergencies. Our modal administrations have decades of experience in responding to all kinds of emergencies—floods, hurricanes, blizzards, blackouts and hazardous material spills. This operational expertise will remain an essential ingredient in our Nation's emergency response capability, and this "all hazard" approach is consistent with the National Response Plan currently under development.

In this post-September 11 world, security has become a prerequisite to the development of an effective transportation system. Just think, for example, about how many fewer people might be flying today were it not for the decisive steps that were taken in the months after September 11 to tighten security throughout our Nation's aviation system. The Department of Transportation continues to support the development of intelligent security policies. If it is not secure, then it is not safe and will not be good for our economy.

Thank you very much for the opportunity to appear here today. I look forward to answering your questions.

Senator LOTT [presiding]. In Senator McCain's absence, Senator Hollings and I will just keep the testimony moving. So I believe Admiral Thomas H. Collins, Commandant of the U.S. Coast Guard, we'll be delighted to hear from you.

STATEMENT OF ADMIRAL THOMAS H. COLLINS, COMMANDANT, DEPARTMENT OF HOMELAND SECURITY, U.S. COAST GUARD

Admiral COLLINS. Thank you, Senator, distinguished Members of the Committee. I appreciate the opportunity to discuss our accomplishments in improving maritime security since September 11, 2001, and additional measures we need to further promote our maritime security.

I am very, very pleased to share the panel with my colleagues from Department of Homeland Security and Department of Transportation. I'm also grateful for the review and insight provided by the General Accounting Office, and look forward to their continuing recommendations to enhance our maritime safety program initiatives.

Now, working within the Department of Homeland Security, the Coast Guard's plan to reduce maritime security risks involves building capacity, capability, partnerships in four distinct but interrelated areas. The first is enhancing what we call "maritime domain awareness"; second, creating and overseeing a maritime security regime for this nation; three, increasing our operational presence and enhancing deterrence; and, four, improving our response posture as an organization. And I'd like to briefly highlight some of the select few accomplishments in each of these areas.

First, maritime domain awareness. We define that as having—ideally, the ultimate state—as having comprehensive information, intelligence, and knowledge of all relevant entities and activities in the maritime domain that would or can impact America's safety, security environment, and the economy. We've been very, very busy in this area enhancing our ability to move toward that end state. Now, we've established a formal intel program in our organization. We have improved our command-control communications capability, connectivity, and interoperability. We're requiring vessels entering our ports to provide 96-hour advanced notice of arrival, and then tracking and screening vessel arrivals—people, cargo, and vessels. We've established field intelligence support teams and increasing our collection and analysis capability, and aggressively pursuing systems that will give us greater visibility in the maritime environment, namely integrated Deepwater systems and Rescue 21 projects.

In the second area, maritime security regime, we are very, very pleased with the progress that we have made in implementing the

terms and conditions of the Maritime Transportation Security Act of 2002. In a parallel effort, we have driven through IMO, a brand new international security regime for international ports and ships, in about a year's time-frame. I think that's quite an accomplishment. And we've issued interim rules in July 1, 2003, to implement MTSA and are on target to provide the final rules in October of this year.

We've also completed 13 port security assessments, of a total of 55, and by the end of calendar year 2004 we will complete those formal port security assessments through the 55 ports. And we've increased information sharing, at the national, state, and local level, with industry.

The third area, operational presence. With the help of Congress and the support of the President and our Secretary, we have increased the capacity and the capability of the Coast Guard to have a increasing presence in our ports and waterways. We've created four maritime safety and security teams. Two more will be in place this fall, six more in the fiscal 2004 budget, for a total of 12. We've provided armed security boardings and onboard escorts of high-interest vessels, and enhanced our control of vessels, with escorts and sea marshals. And we've added new patrol boats and people to our inventory.

In the fourth area, our response posture, we're reconstituting the chemical, biological, and radiological dispersal program within our service and enhancing the strike-team capabilities that we maintain.

Now, these security measures in these four areas we've instituted so far have had no significant adverse impact on maritime commerce. That said, the regulatory impact of MTSA on the maritime industry will be significant, affecting over 10,000 domestic vessels and 20,000 foreign vessels, 5,000 maritime transportation facilities, and 40 offshore platforms. And the timeline for implementing the new requirement is exceptionally short. The regulation would be fully implemented by July 1, 2004. We estimate the cost to industry to be $1.5 billion in the first year and $7.3 billion over the next 10 years.

We are making good use of the resources we received in Fiscal Year 2002 and 2003, and the planned resources for Fiscal Year 2004. We have had outstanding support from the Administration and from Congress in this regard. A lot has been accomplished, but we still have a long way to go.

We're working diligently to increase maritime security by building a layered defense approach to maritime security by recapitalizing our Deepwater assets, by identifying and addressing vulnerabilities revealed by port security assessments, by putting a comprehensive planning and exercise scheme in place throughout the country, and monitoring foreign compliance with plan certification, as required by MTSA.

Mr. Chairman, we have a solid plan for maritime security, and we are executing it. All of our efforts, again, are designed to build the necessary authorities, the necessary capability, the necessary capacity, and the necessary partnerships to mitigate maritime security risks to our Nation. To achieve these goals, we need support for our 2004 budget, continuing a phased approach to building out

these capability and capacity. We need support for our 2004 authorization bill. It provides necessary authority we need to protect our vital infrastructure and respond quickly, if necessary, and it adds ability for us to enforce laws ashore in proximity to the waterfront.

Thank you for the opportunity to testify before you today, and I'm happy to answer questions at the appropriate juncture. Thank you.

[The prepared statement of Admiral Collins follows:]

PREPARED STATEMENT OF ADMIRAL THOMAS H. COLLINS, COMMANDANT, DEPARTMENT OF HOMELAND SECURITY, U.S. COAST GUARD

Good morning Mr. Chairman and distinguished Members of the Committee. It is my pleasure to be here today to discuss the Coast Guard's accomplishments in improving maritime transportation security since the terrorist attacks of September 11, 2001, the impact of those accomplishments on maritime commerce, and the additional measures that may be needed to further promote maritime transportation security.

The attacks of September 11, 2001, have required the United States and the world to recognize how vulnerable our international systems of transportation and trade are to those who intend to do us harm. A terrorist incident against our marine transportation system would have a serious and long-lasting negative impact on global shipping, international trade, and the world economy. Our ports and waterways also have significant strategic military value. Valuable and vulnerable . . . these factors make protection of our marine transportation system a high priority in the U.S. Maritime Homeland Security Strategy.

Accomplishments

Working in concert with the Department of Homeland Security and its agencies, we developed a strategic approach to maritime security that places a premium on identifying and intercepting threats well before they reach U.S. shores. We will do this by conducting layered, multi-agency, maritime security operations; strengthening the port security posture of our strategic economic and military ports; building on current international cooperative security efforts; and making risk-based decisions. These key elements form the basis of the Maritime Homeland Security Strategy, closely aligning with the President's National Strategy for Homeland Security. This is a sound strategy that reduces maritime security risks through: (1) increasing our maritime domain awareness; (2) implementing preventative measures to detect and deter; (3) securing our borders and protecting vital infrastructure; and (4) preparing to respond quickly if necessary.

Since the attacks of September 11, 2001, the Coast Guard has instituted measures to increase maritime domain awareness—a combination of intelligence, surveillance, and operational information to build as complete a picture as possible to the threats and vulnerabilities in the maritime realm. Within 30 days of the attacks, we amended our regulations to require ocean-going vessels approaching U.S. to provide advance notice 96 hours prior to arrival at U.S. ports. We also centralized reporting from individual Captains of the Port to a single location to enable better coordination and analysis of information and more rapid dissemination to other agencies. The Coast Guard Intelligence Coordination Center, co-located with the Office of Naval Intelligence at the National Maritime Intelligence Center in Suitland, Maryland, established COASTWATCH, a process that analyzes these notice of arrival reports using law enforcement and intelligence information and reporting vessels of interest so that Coast Guard and other agencies could appropriately respond to board those vessels before they reached port, if necessary. The Coast Guard continues this practice today and has improved electronic sharing of notice of arrival reports and accompanying intelligence information with Bureau of Customs and Border Protection (CBP), Transportation Security Administration (TSA), Information Analysis and Infrastructure Protections (IAIP) Directorate, Department of Defense, and other components of the Intelligence Community.

Recognizing the criticality of intelligence in achieving maritime domain awareness, we have taken several key steps to grow our intelligence program. Last year we elevated the Director of Intelligence to an Assistant Commandant level to align with the importance I place on intelligence to support Coast Guard operations. Additionally, we are in the process of completing the measures required to fully implement the December 2001 legislation adding the intelligence element of the Coast

Guard to the U.S. Intelligence Community. Our primary focus on this point has been to meet the stringent legal and oversight requirements that accompany Intelligence Community membership as we begin to build better collection and analytical capabilities. We are able to provide more information on this initiative in a classified briefing. Within the last 6 months, the Coast Guard has transformed the existing Atlantic and Pacific Area intelligence staffs into Maritime Intelligence Fusion Centers Atlantic and Pacific. This change increased collection and analytical capabilities to enhance all-source fusion of intelligence and information and to improve the timeliness and quality of theater level intelligence support to Coast Guard operational forces. The new Maritime Intelligence Fusion Centers also ensure rapid reporting of information gathered by Coast Guard forces into the IAIP Directorate and Intelligence Community at the national level. We have established Field Intelligence Support Teams, consisting of Coast Guard intelligence analysts and Coast Guard special agents, to provide tactical intelligence support to Coast Guard Captains of the Port through collection and reporting of suspicious or criminal activity in the port areas, to share information with other agencies at the local level, and to rapidly disseminate intelligence to the Captain of the Port and other local commanders.

The regulations which implement the Maritime Transportation Security Act of 2002 (MTSA) require certain vessels to install an Automatic Identification System (AIS) by the end of 2004, and the Coast Guard will install AIS capabilities at each Vessel Traffic Service location nationwide with the long-term goal of National AIS coverage. Additionally, the Coast Guard has completed port security assessments at 13 of the 55 most significant military and economic ports in the United States and will complete the assessments of all 55 ports by the end of calendar year 2004. These assessments are unique because they capture information from local law enforcement sources not previously shared with intelligence, thus making them more comprehensive. Finally, the Coast Guard continues to coordinate maritime security information sharing, consistent with the MTSA requirements, at the national level with other agencies, and at the local level with federal, state and local entities and with industry. Because the maritime industry has not organized itself to receive and send information regarding threats and vulnerabilities to maritime critical infrastructure as discussed in PDD 63, the Coast Guard formed a maritime information sharing process to share threat information with the maritime industry and to receive reports of suspicious activities from them.

Terrorist activities and threats, coupled with our own acknowledged vulnerabilities, prompted unprecedented multi-lateral security activities over the past two years. The United States, working in concert with our trading partners, adopted a landmark international maritime security regime through the International Maritime Organization. This approach minimized the potential for a proliferation of national, unilateral security requirements that could impair maritime commerce, while at the same time ensured that meaningful security measures will be consistently implemented on a global scale. More specifically, on December 13, 2002, over 100 nations at IMO adopted amendments to the International Convention for the Safety of Life at Sea (SOLAS) and an International Ship and Port Facility Security (ISPS) Code. On November 25, 2002, President Bush signed the MTSA. In passing the MTSA, Congress expressly found that it is in the best interest of the United States to implement the security system developed by IMO because it contains the essential elements for enhancing maritime security. Both of these important instruments—the SOLAS security amendments and the MTSA—are major steps in addressing maritime security, and together they form the cornerstone of the nation's maritime homeland security strategy.

In coordination with the Transportation Security Administration, Maritime Administration, and Bureau of Customs and Border Protection, the Coast Guard, as the lead Federal Agency for maritime security, published regulations on July 1, 2003 to implement the core security requirements of the MTSA consistent with the SOLAS amendments and the ISPS Code. And these regulations are essential to promote our national strategy of preventing terrorist attacks in the United States, to reduce our vulnerability to terrorism, and to minimize the damage and permit quick recovery from any attacks that might occur. The regulatory impact on the maritime industry will be significant—affecting over 10,000 domestic vessels, 20,000 foreign vessels, 5,000 marine transportation related facilities and 40 critical offshore platforms—and the timeline for implementing the new robust maritime security requirements is exceptionally short—the regulations will be fully implemented by July 1, 2004.

Among other requirements, the regulations compel regulated vessels and facilities to conduct security assessments and to develop detailed security plans that address vulnerabilities revealed by those assessments. The regulations contain requirements for the designation and competency of security personnel, including standards for

training, drills, and exercises. The regulations further delegate authority to Captains of the Port to conduct Area Maritime Security Assessments and to develop Area Maritime Security Plans for their respective port areas. This "family of plans" approach establishes a layered system of protection that involves all maritime stakeholders and will be consistent with National Maritime Transportation Security Plan being developed in cooperation with the Transportation Security Administration, the Bureau of Customs and Border Protection, and other agencies.

For vessels subject to the SOLAS amendments and the ISPS Code, the Coast Guard is implementing strong Port State Control measures to aggressively ensure foreign vessels have approved plans and have implemented adequate security standards. The measures include tracking performance of all owners, operators, flag administrations, recognized security organizations, charterers, and port facilities. Noncompliance will subject the vessel to a range of control measures, which could include denial of entry into port or significant delay. This aggressive Port State Control regime will be coupled with the Coast Guard's Foreign Country Security Audit program that will assess both the effectiveness of anti-terrorism measures in foreign ports and the foreign flag administration's implementation of the SOLAS amendments and the ISPS Code.

In addition to adopting the landmark SOLAS amendments and publishing comprehensive regulations implementing MTSA, the Coast Guard has successfully implemented other measures to increase maritime homeland security. The Coast Guard has increased port security in the nation's most important economic and military ports through the use of:

- more patrols by aircraft, ships, and boats;
- more escorts of passenger ships;
- armed security boardings;
- and onboard escort of high interest vessels (vessels with cargoes, crewmembers or other characteristics that warrant closer examination, arriving at or departing from U.S. ports)
- the creation and enforcement of hundreds of security zones in and around critical infrastructure;
- and the establishment of six Marine Safety and Security Teams (MSSTs) (a highly specialized quick response force capable of rapid, nationwide deployment via air, ground or sea transportation in response to changing conditions and evolving Maritime Homeland Security mission requirements.

Additionally, our Strike Teams, which were instrumental in response to the Anthrax attacks at the Hart Senate Office building, are being trained to respond to a CBR attack. We have also begun recapitalization of our Deepwater assets. Homeland Security necessitates pushing America's maritime boarders outward, away from the ports and waterways, so integrated, maritime operations can be implemented. Deepwater provides this capability while developing a far more robust and effective MDA system.

We also have not acted alone. At the field level, Coast Guard Investigative Service agents and Field Intelligence Support Teams directly liaise with their TSA, CBP, and ICE peers to collect and share operational intelligence. Coast Guard and TSA personnel are working together with the Port of Miami to facilitate cruise ship passenger and baggage screening. At the policy development level, an Underwater Port Security Working Group comprising representatives of the Coast Guard, TSA and the U.S. Navy has been established to implement promising technologies to mitigate underwater homeland security threats. Additionally, a Radiological Dispersal Device/Improvised Nuclear Device Working Group, consisting of representatives from 16 government agencies and departments, has been established for deterrence and detection of nuclear smuggling into or within the United States. These are just a few examples of how we have actively sought out and leveraged inter-agency partnership to provide a defense in depth.

Effect on Commerce

The Coast Guard is sensitive to the impact that increased security may have on commerce. The wide variety of security measures implemented to date has had no significant adverse impacts on the flow of maritime commerce. That said, we note that the cost to industry of the MTSA implementing regulations is estimated to be $1.5 billion in the first year and $7.3 billion over the next 10 years. While we clearly understand that the cost of these security regulations to the maritime industry is not insignificant, a terrorist incident against our marine transportation system would have a devastating and long-lasting impact on global shipping, international trade, and the world economy. As part of a recent port security training exercise,

a maritime terrorist act was estimated to cost up to $58 billion in economic loss to the United States. Thus, the cost is outweighed by the mitigation of risk to the industry. We have, however, developed the security regulations to be performance-based, providing the majority of owners and operators with the ability to implement the most cost-effective operational controls, rather than more costly physical improvement alternatives. The Coast Guard will be vigilant in its Maritime Homeland Security mission and will remain sensitive to the impact of security measures on maritime commerce.

Additional Measures

We do note that, since September 11, 2001, we have increased our uniformed presence ashore at waterfront facilities and critical infrastructure adjacent to the marine environment. Immediately after September 11, 2001, however, we identified a gap in our authority ashore and developed a proposal to close that gap. Although, the Coast Guard is at all times an armed force and has broad authority to protect waterfront facilities and other shore installations under a number of statutes, such as the Maritime Transportation Security Act, the Ports and Waterways Safety Act, and the Espionage/Magnuson Act, we lack express authority to arrest a person who commits a Federal offense on shore and to carry a firearm ashore in the performance of official law enforcement duties. Clarifying this authority remains a top legislative priority for the Coast Guard, and we greatly appreciate the inclusion of legislation addressing this matter in the pending Coast Guard Authorization bill, S. 733. This authority is not included in the House version of the bill and H.R. 2443, and we appreciate the Senate's support in including this provision at conference.

The United States Coast Guard has and will continue to take a leadership role in coordinating the multi-agency, public, and private, national and international maritime security effort as part of the Department of Homeland Security's larger national Transportation System Security Plan. The men and women of the Coast Guard are committed to the continuing protection of our nations. Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.

Senator LOTT. Now, let's see, Mr. Bonner, thank you very much—Commissioner of Customs and Border Protection. If you would go ahead.

STATEMENT OF HON. ROBERT C. BONNER, COMMISSIONER, CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BONNER. Thank you, Senator Lott and Senator Hollings, other distinguished Members of the Committee. I want to thank you and the Chairman for the opportunity to discuss what U.S. Customs, now U.S. Customs and Border Protection, has been doing since 9/11 to protect the American people and to better secure our borders, the borders of our country and all of our ports of entry into our country, through which, as you know, all people and vehicles and goods must pass.

First of all, I want to say I'm very delighted to be on this panel with my colleagues, Admiral Loy and Admiral Collins, as well as Under Secretary Shane and others. And suffice to say that Customs and Border Protection has been and continues to coordinate on many issues with the Coast Guard and with TSA, and that coordination has been and will be facilitated by the fact that all three of these significant agencies of the Department of Homeland Security are now in one department, the Department of Homeland Security.

Let me say it's—you know, it's an understatement to say that before the terrorist attacks at our border, and particularly our transportation systems were designed not for security but for the rapid movement of people and commerce. And it has been our challenge, collective challenge, since 9/11 to essentially retrofit the global sys-

tem of commerce to protect the American people from terrorism and yet to do that in a way that it does not unduly impede and, where possible, actually facilitates a more efficient flow of legitimate trade and people.

I want to just take a moment to talk about U.S. Customs and Border Protection, for just a brief moment, because it is a new agency that was formed on March 1 of this year by merging most of U.S. Customs with the immigration inspectors and the border patrol from the former INS and the agriculture inspectors from the Department of Agriculture.

Now, since March 1 of this year, for the first time in our country's history, there is one agency responsible for managing and securing the U.S. border and all of the 300-plus ports of entry into the United States. And by unifying the border agencies, we are more effective, certainly, than we were before March 1, before the Department of Homeland Security was created, when we were fragmented, literally fragmented. The border management and security effort was fragmented between four different agencies and three different departments of government—Immigration, Customs, Agriculture Inspectors, and Border Patrol.

The unification of Customs and Border Protection was vehemently demonstrated at Dulles International Airport last week, when Secretary Ridge introduced the new CBP officer position, or Customs and Border Protection inspectional officer position, and the new Customs and Border Protection uniform—one uniform for all Customs and Border Protection inspectors, the inspectional work force, at all of our ports of entry—as well as one new Customs and Border Protection inspectional officer, rather than the legacy Customs inspectors, Immigration and Agriculture inspectors. And we'll start with the new CBP officer by training a new cadre of front-line inspectors, Customs and Border Protection officers, to handle essentially all primary and secondary inspections for all purposes. And we'll also be deploying some agriculture specialists to perform the specialized agriculture specialty inspection functions.

Now, let me turn to the securing of our border, because securing of our border involves something more than just our physical border, either land border or seaports or international airports. It includes the notion of extended border, of a defense and depth strategy where Secretary Ridge has sometimes called it a "smart border." And that means we want our border to be the last line of defense for the American people, not the first line of defense. And our strategic approach to secure the flow of cargo and people is multilayered, and it starts in many places. It starts as far away, by the way, as Central Asia where Customs and Border Protection personnel are working with our foreign partners to interdict special nuclear materials at or near their source. It extends, certainly, to the foreign loading docks and the more secure supply chains of our customs and trade partners in the Customs-Trade Partnership Against Terrorism. And it extends literally to the terminals of foreign ports, where we are—under the Container Security Initiative, which we have in place, where Customs and Border Protection officers are working with their foreign counterparts to target and in-

spect high-risk containers before they go onboard vessels headed for the United States.

These extended border efforts are key components of Customs and Border Protection's multilayered strategy for securing our border, yet also, at the same time, facilitating the more efficient flow of legitimate goods and people into our country. And it's important to note, if I could, that these programs have been implemented—and they've been implemented, every program I just mentioned, since September 11, 2001. CSI is now operational in 16 foreign seaports around the world, and we're continuing to expand it. And, that said, we have much work to do to get CSI fully operational.

And with respect to the Customs-Trade Partnership Against Terrorism, over 4,000 companies are enrolled in C–TPAT, most major U.S. importers, but also major air, sea, rail, and trucking carriers, as well as domestic port and terminal operators. And we have opened C–TPAT to foreign manufacturers for the first time last month.

Now, I just want to touch on one other thing before I close, and that is what we're doing at the U.S. ports of entry to protect the American people and prevent terrorists and terrorist weapons from entering the country. And that's our priority mission at Customs and Border Protection, preventing terrorists and terrorist weapons from entering the United States.

First of all, we use risk-management techniques to identify and screen the relatively few high-risk cargo containers of the millions—actually, if you take sea containers, almost 7 million containers that come into the U.S. annually. But, that said, in the last 2 years—if we go back 2 years ago, only 9 percent of all rail containers were inspected when they crossed the border into the U.S. That figure is now 22.6 percent. Two years ago, we inspected only 2 percent of the sea containers coming into the U.S. We now inspect 5.2 percent. The truck inspections have increased from 10.3 to 15.1 percent over the last 2 years. And, overall, if you look at all containers, no matter what the mode is, entering the United States, the Customs and Border Protection is inspecting, currently, approximately 12.1 percent of all cargo containers entering the United States. And that's up from about 7.6 percent 2 years ago.

But we're doing it not just on a random basis, but we're doing it on a targeted basis based upon advanced information we have to identify the high-risk containers, because that's the key. And we've gotten this advance information through such things as the 24-hour rule, which we have implemented, to get advance information about cargo containers before they arrive in the United States; in fact, 24 hours before they leave the foreign ports destined for the United States. And we're doing that through getting advance passenger information about all people flying into the United States, as well as under the proposed Trade Act of 2002 regulations, which will require advance information with respect to all shipments, irrespective of the mode of transportation—rail, air, truck. And it's through effective targeting that we can and we are meeting our goal of inspecting 100 percent—because that's our goal—of all of the high-risk cargo and people while, at the same time, allowing legitimate commerce and passengers to proceed unimpeded.

And our inspection rates have gone up, because, among other things, we have been able to deploy more sophisticated detection equipment, like large-scale X-ray machines. I know, Senator Hollings, you've seen some of these at the Port of Charleston. But we've increased the number of large-scale X-ray machines that can screen whole containers. From about 45 on 9/11 of 2001, we now have increased that by 200 percent; we have 135 of these large-scale containers, and they are deployed at our northern border major crossing points, commercial entry points, and at our seaports, and they weren't on September 11, 2001.

So let me just say, in closing, that Customs and Border Protection has moved aggressively to secure the flow of trade and commerce into our country, and people into our country. And it's done it at our physical border, and it's done it beyond our physical borders, working both with foreign governments and the private sector. And it has done that without materially slowing down the flow of legitimate commerce and trade.

We're, by no means, finished yet, but I can say that America is safer and our borders are more secure, substantially more secure, than they were on 9/11/2001. And I look forward to working with Secretary Ridge, Under Secretary Hutchinson, Admiral Collins, Admiral Loy, and with this Committee to continue our project of securing America from international terrorism.

Thank you.

[The prepared statement of Mr. Bonner follows:]

PREPARED STATEMENT OF HON. ROBERT C. BONNER, COMMISSIONER, CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Chairman McCain, Senator Hollings, Members of the Committee: Thank you for the opportunity to testify today to discuss what U.S. Customs and Border Protection has been doing since September 11, 2001 to protect the American people, and to better secure the borders of our Nation and its ports of entry, through which all people, vehicles and goods must enter. This includes the systems by which people and goods move into and out of our country.

First, I want to say how delighted I am to be here with Admiral Loy and Admiral Collins. CBP has coordinated on many issues with the Coast Guard and with TSA, as this coordination has been facilitated by the fact that all three agencies are now within the Department of Homeland Security. Indeed, TSA and CBP are agencies within the Border and Transportation Security (BTS) Directorate of the Department, which, under the leadership of Under Secretary Asa Hutchinson, has assisted greatly in our coordination efforts.

It is an understatement to say that, in the days before the terrorist attacks, our border systems were designed, not for security, but for the rapid movement of people and commerce. It has been our challenge since September 11 to "retrofit" this global system of commerce to protect the American people from terrorism—and do it in a way that does not impede, and indeed, where possible, facilitates, the efficient flow of legitimate people and goods so vital to our economy, and the economy of the world.

CBP Transition

Before I go further, however, I want to spend a few moments talking about U.S. Customs and Border Protection—or "CBP." As I am sure all of you know, CBP was formed on March 1, 2003 through the merger of most of the U.S. Customs Service with the immigration inspectors and U.S. Border Patrol of the former INS and the agricultural border inspectors of the USDA. Although under the Homeland Security Act and the Department's Reorganization Plan, CBP is the successor agency to U.S. Customs, CBP is very much a new agency within the Department of Homeland Security. Now, for the first time in our Nation's history, there is a *single* U.S. border agency, CBP—responsible for managing and securing the entire U.S. border, that is, all of the 300 plus ports of entry, and between the ports of entry. And, through the unifying of customs, immigration, and agriculture functions at the border, under

one unified chain of command, we are more effective than we were before March 1, when we were fragmented into 3 agencies in 3 different departments of government.

This was most vividly demonstrated last week, when Secretary Ridge, Under Secretary Hutchinson, and I were at Dulles Airport, introducing the new "CBP Officer"—with a new CBP Officer's uniform and DHS/CBP patch—to the American people. Starting this October, we will no longer be training legacy "immigration" or "customs" inspectors. We will be training a new cadre of "CBP Officers," who will be equipped and trained to handle all CBP primary and secondary inspections, for all purposes in the passenger environment. These CBP Officers will also perform all primary inspection functions in the cargo environment, although we will also be deploying CBP Agriculture Specialists to perform more specialized agricultural secondary inspection functions.

And current legacy immigration and customs inspectors have already begun cross-training. So, we're not waiting for the new "CBP Officers" to graduate from FLETC to begin creating "one face at the border." We have already begun to roll out unified CBP primary inspections at our international airports, and we are merging our specialized immigration and customs anti-terrorism secondary and passenger analytical targeting units. In short, we are moving out quickly to achieve the President's and the Secretary's goal of "One Face at the Border," that is one unified, flexible, and effective agency to manage and control our Nation's borders.

This merger has allowed us to think comprehensively about how we better secure, manage and facilitate the movement of people and commerce into and out of our country. No longer is our government fragmented—with one agency thinking about the movement of people, another thinking about cargo, and still another thinking about agriculture protection. It's one agency focusing on the whole picture at our borders.

"Beyond the Border" Initiatives

And in our view, that picture does not begin at our land border or the U.S. water's edge. We view our border as the last line of defense for the American people, not the first line. Our effort to secure the flow of people and cargo is many layered, and starts in many places—in Central Asia, where CBP personnel are working with foreign partners to interdict WMD material at its source. At the factory floors and in the secure supply chains of our partners in the Customs-Trade Partnership Against Terrorism, or C–TPAT. At the docks of our Container Security Initiative, or CSI, ports around the world, where CBP officers are working with our foreign counterparts to target and inspect high-risk containers *before* they are shipped to the United States. In Canada and Mexico, with the people and companies we vet through the FAST, NEXUS, and SENTRI programs. To ensure that our foreign counterparts have the right skills and capabilities to cooperate successfully, we also provide training and technical assistance when needed.

And we also apply the "beyond the border" concept to targeting and interdicting high-risk people before they head to the United States. In fact, just a couple of weeks ago, CBP targeted two passengers traveling from Paris to Chicago who used a route typical of an individual trying to enter the U.S. with fraudulent documents. Because we were able to target these people before they got on the plane in Paris, we were able to enlist the air carrier to deny boarding to these individuals—who were a threat as the documents they were using were fraudulent.

These "beyond the border" efforts are key pieces of CBP's layered strategy for protecting the American people from terrorism, while facilitating the efficient flow of legitimate people and goods into our country. These programs are being implemented and have been effective. In the short life of CSI, we have already worked with our foreign partners to intercept and seize shipments that posed a potential threat to the American people—including machine guns, gas masks, and other military equipment that would clearly be on Al Qaeda's shopping list. And CSI is now operational in 16 seaports around the world—in Europe, Asia and Canada. Once all the ports in Phases 1 and 2 of CSI become operational, approximately *80 percent* of the 7 million maritime containers heading for the United States annually will be under the CSI blanket. That said, we still have much work to do to get CSI fully operational.

It is also important to view CSI in the context of CBP's layered-defense strategy. Just as important is our effort to secure the supply chain through C–TPAT. Currently, over 4,000 companies are enrolled in C–TPAT—not only U.S. importers, but also all the major air, sea, rail, and trucking carriers, a large number of brokers and forwarders, and domestic ports and terminal operators. And on August 18, we opened C–TPAT for the first time to foreign manufacturers—first those based in

Mexico, to facilitate their participation in the FAST program, and then to a select group of manufacturers based in other parts of the world.

While CSI protects one means of moving goods into the country at a particular place—the foreign seaport—C–TPAT protects the entire supply chain, including goods moving across our land border by truck or rail and both sea and air cargo. Our C–TPAT partners are making great strides to secure every link in their supply chains. And, we are working with our C–TPAT partners to redesign the containers themselves—adding sophisticated technology to make them "smarter," more secure, and tamper-evident. In short, we are in the process of revolutionizing and retrofitting global trade to face the 21st Century terrorist threat.

And, we are validating that the security measures have been taken. We've launched a program to send teams of CBP Supply Chain Specialists around the world to verify that our C–TPAT partners, their suppliers, and logistics vendors are doing what they say they are doing.

I've spent a great deal of time focusing on what we are doing "beyond the border." But before I close, I should touch on what we are doing *at* U.S. ports of entry to protect the American people and prevent terrorists and terrorist weapons from entering the United States.

First, let me speak to the numbers. Two years ago, when I took over as Commissioner of Customs, 7.6 percent of all containers entering the United States—by land, sea, or rail—were inspected by Customs. That figure is now up to 12.1 percent, and it is rising. Two years ago, only 9 percent of all rail containers were inspected. That figure is now 22.6 percent. Sea container inspections have increased from 2 percent to 5.2 percent. And truck inspections have increased from 10.3 percent to 15.1 percent. These are impressive numbers, and, where necessary, I am pushing to increase CBP's capacity to rapidly inspect containers without slowing legitimate trade.

Advance Information and Technology

I should point out there is no reason to increase the inspections blindly—or just for the sake of having higher inspection statistics. Quite frankly, it would be counterproductive and damaging to the U.S. economy to inspect 100 percent of the 7 million sea containers or the 11 million trucks that arrive in the United States every year. We must use some risk management techniques to identify and screen the relatively few high-risk shipments out of the millions of virtually no-risk shipments.

Through regulations such as the 24 Hour Rule, those requiring advanced passenger information, and the proposed rules under the Trade Act of 2002 which require advance information on all shipments, I am pushing to improve our ability to focus our efforts on the high-risk shipments. We are also working with the Intelligence Community and others to improve our targeting rules and systems. It is through effective targeting that we meet our goal of inspecting 100 percent of high-risk people and cargo, while allowing legitimate commerce and passengers to proceed unimpeded.

We are also increasing our inspection rates through the rapid deployment of radiation detection technology, as well as large-scale X-ray type imaging systems. In the almost two years since I became Commissioner of Customs, CBP has deployed this equipment to every major U.S. port of entry. This has dramatically increased our ability to inspect high-risk containers, but it has done so in a way that does not interrupt the flow of legitimate commerce.

In closing, CBP has moved aggressively to secure the flow of people and commerce into our country. It has done this at our physical border, and beyond our border—working both with foreign governments and the private sector. And it has done this without materially slowing the flow of legitimate travel and commerce. Are we finished yet? No. Are we working to make America even more safe? Yes. And I look forward to working with Secretary Ridge, Under Secretary Hutchinson, Admiral Loy, and Admiral Collins—as well as this Committee—to continue our project of securing America from terrorism.

Senator LOTT. Admiral Loy?

STATEMENT OF ADMIRAL JAMES M. LOY, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral LOY. Good morning, Senator Lott, Senator Hollings, Committee Members. I'm pleased to have this opportunity to appear before you and report on TSA's progress and plans for improving security in the Nation's transportation system and to discuss

the recommendations that we have all seen in the reports from the General Accounting Office.

I, too, enjoy the opportunity to sit at this table with Tom Collins and Rob Bonner and Jeff Shane. These folks work daily, weekly, monthly with all of us at TSA in the efforts to secure the transportation system. It is always a personal pleasure to work with them then and to be with them here today and report back to this Committee.

Under the leadership of Secretary Ridge and Under Secretary Hutchinson, we have forged working partnerships throughout the Department. We continue to work closely with the operating administrations in the Department of Transportation, especially TSA does. They provide another vital link with the transportation providers, and we communicate daily to share expertise, to ensure that we make the best use of each organization's resources and opportunities in our mutual reach to the stakeholders throughout the transportation system.

As we near the second anniversary of the terrorist attacks on our country that forever changed our sense of security in today's world, I feel confident in assuring you and the American people that the civil aviation sector and the larger transportation sector is more secure today than it has ever been, and it will continue to become even more secure as we mature our complementary systems of systems.

Today, I'd like to take just a moment to review some of the major strides that we've made in aviation security and our action plan for making further improvements. TSA is working with the other DHS agencies and DOT operating administrations to develop security standards and initiatives to create a more uniform level of security across all transportation modes; again, as both my colleagues, in advance, have said, without impeding travel or commerce, which has, for all intents and purposes, become one of those inalienable rights that the Founding Fathers were talking about but didn't perhaps say it so clearly.

First, let me respond to a concern this Committee voiced the last time I testified. It's off the mission point, but, I think, very germane to this brand new agency that was created by the Congress.

The Chairman, on that occasion, challenged me, specifically, to pay particular attention to financial management and contract oversight. NCS Pearson stories were in the air, and you suggested the reputation of a brand new agency could get labeled very quickly in one direction or the other. And the Pearson audit will run its course very shortly, and we will deal with it as we have to. And we'll finally put that saga behind us.

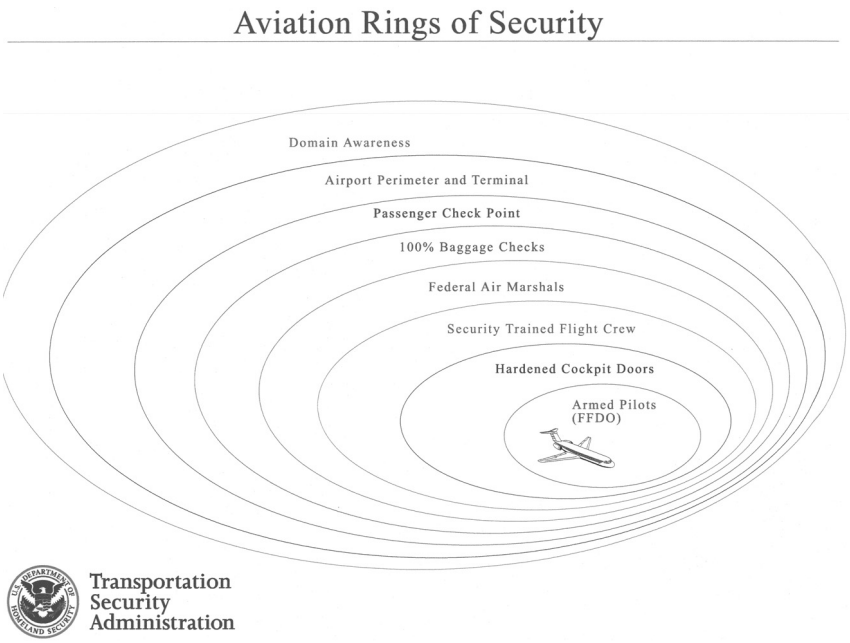
But, in the meantime, we've taken that challenge from this Committee very seriously. We've hired an excellent team of acquisition professionals and have designed first-class systems of program management. Investment review boards, constant contract oversight, is the routine of the day at TSA. And I can show the Committee, and will be happy to, dozens of major contracts, on time and on budget. The TSA was just notified of our clean-audit status just this last month, with every expectation that we'll hold onto that status as the Fiscal Year closes. That is virtually unheard of

for a brand new agency, especially one that inherited some very serious property issues at our inception.

But I'm proud of what we accomplished in this area, and I want the Committee to know that one of our strategic goals is organizational effectiveness, and we took seriously your commentary as we continue to take seriously our mission-related ones, as well.

Mr. Chairman, I, too, will submit my written testimony for the record and discuss our short but productive history from a couple of charts, and the Members each have copies in front of them.

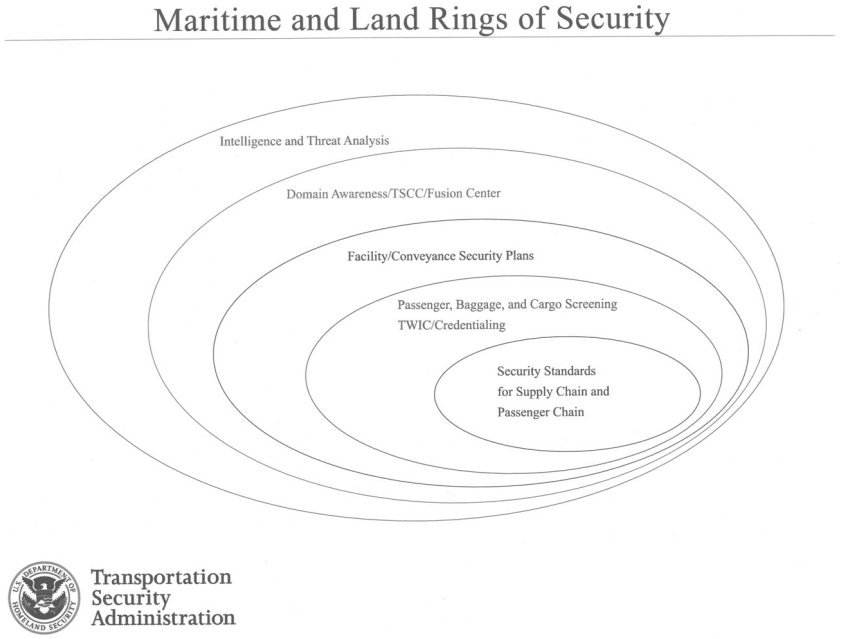
The first one shows a system of systems that we've built as the foundation of security at our airports. We've looked hard for the silver bullet and found that none existed. And our default plan has become, as you've heard from the other speakers so far, a concept where we had to build a system of systems to build the adequate approach to aviation security. And the concepts and specific programs you see depicted as concentric ellipses on this chart begin out there when we're gathering information, and end literally in the cockpit of each passenger-carrying airliner in this country.



We leveraged these systems with CAPPS I, a system that we have in place at the moment that we want very much to replace with CAPPS II. Each is really a scalable dynamic that is keyed to the alert conditions system run by the Department of Homeland Security. But our notion is simply to take advantage of the law of aggregate numbers by sequencing these systems' elements as a series of obstacles any terrorist would have to clear in order to accomplish his objective. Each of these elements has been carefully developed with attention both to security and customer service and minimum impact on the flow of commerce. I'm happy to try to answer questions on any of these elements in the Q&A, but they each

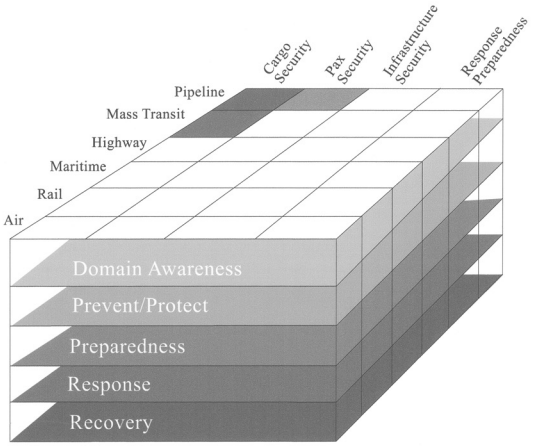
have prompted wide commentary as they have come into practice, and they were built and put into the system each for very, very good reasons.

The second chart is more notional as it defines the shift that is actually taking place between almost exclusive concentration on aviation security to developing what we need to develop for the rest of the national transportation system. It is a corresponding array of tools or concerns more appropriate to the rest of that system, and it recognizes two simple realities. First, most of our attention, to be sure, energy and resources, have been focused on aviation these past 2 years. And, second, we've learned many lessons as a result, and many of the lessons learned in that work will allow us to take a threat-based risk-managed approach for the rest of the transportation system that will capitalize on industry ownership and a regulatory-compliance approach by TSA. There will be no need for hundreds of TSA operators like we see at airports; rather, an adequate cadre of policy analysts and a solid group of trained compliance inspectors will be what's necessary to ensure accountability in this system.



The last chart depicts work accomplished and work still to be done. If I can look at it just for a second with you, I would like to offer some commentary on what we're trying to do here.

National Transportation System Security Plan (NTSSP)



Transportation Security Administration

If you look at just the face, the upper face, of this cube, a classic Rubik's cube of attempting to develop the transportation system security plan, you can see, aggregated down the lefthand side, what I feel are the six main elements of our national transportation system. A lot of attention has been given to air up front. Rail, maritime, highway, transit, and pipeline deserve attention such that none of them are perceived by the bad guys as a weak link in that system.

If you look across the base of that upper level, whether we're talking about cargo or people, in the form of passengers or crew, or infrastructure security or the notion of response preparedness, the face of that cube is really about understanding the entirety of the national transportation system. And in today's parlance of computer technology, if we click on the face of any one of those upper-level white squares, a couple of blue ones, and a green one, we should be able to look at the intersection between, for example, maritime and cargo, and grapple with what's going on among all the agencies in the Federal Government, in the industry, at state and local levels, and truly in terms of our global partnerships around the world. Out of that should come our sense of vulnerability assessments, of standard-setting, of mitigation strategies, and of some notion of compliance at the other end of the day so that we can report back to this Committee as to how well those things are going across the full face of the transportation sector.

The challenging reality is that the complexity of this chart depicting our approach for just the transportation-security piece is

just that, one puzzle piece in the construct Secretary Ridge and now Under Secretary Libutti, are building to represent the approach to the entire homeland security challenge. Today, we're here to chat with this Committee about the transportation piece.

Mr. Chairman, analysts can point to a veritable obstacle course of challenges to building a comprehensive system of security across all the modes. And while I recognize and respect the difficulty of these challenges, I remain optimistic. We can look, and must look, very positively on the dramatic change in landscape in only the past 2 years. We have learned a lot. We have done a lot.

Mr. Chairman, as my colleagues at this table will attest, this is very hard work. I am blessed at TSA, as I know they are, with people who come to work for us because they were committed to our cause. Everything we've done, we've done with the whole world watching. And I appreciate the intellectual challenges offered by every Member of this Committee at one time or another over the course of the last year. Each time I've visited or talked to you on the phone, I am prodded in my agency to do something better.

Senator Wyden, Senator Dorgan properly challenge us to be satisfied only when we're doing the right things about civil liberties in our CAPPS II project. Senator Hutchison and I have talked long and hard about air cargo and about a registered traveler program. Senator Hollings and I have been discussing port security for 10 years. Senator Burns has made it crystal clear to me where he stands on arming pilots. And I could go on with virtually every Member of this Committee. We are better off as a nation because we challenge each other.

And I want to leave a word of thanks to each of you for your interest and your drive, personally, on these enormously important issues. As Tom said, as Rob said, we have accomplished a lot; we have a lot yet to do.

I'll happily answer your questions when the time is appropriate.

[The prepared statement of Admiral Loy follows:]

PREPARED STATEMENT OF ADMIRAL JAMES M. LOY, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Good morning Mr. Chairman, Senator Hollings, and Members of the Committee. I am pleased to have this opportunity to appear before you today to report on the Transportation Security Administration's (TSA) progress and plans for improving security in the Nation's transportation system and discuss the recommendations of the General Accounting Office (GAO).

Under the leadership of Secretary Ridge and Under Secretary Hutchinson, we have forged working partnerships with other Department of Homeland Security (DHS) organizations. We continue to work closely with the operating administrations of the Department of Transportation (DOT). They provide another vital link with transportation providers, and we communicate daily to share expertise, to ensure that we make the best use of each organization's resources and opportunities.

As we near the second anniversary of the terrorist attacks on our Nation that forever changed our sense of security in today's world, I feel confident in assuring you and the American people that the civil aviation sector and the larger transportation sector is more secure today than it has ever been and it will continue to become even more secure as we mature our complementary "systems of systems."

Today, I would like to review some of the major strides that we have made in aviation security and our action plan for making further improvements. TSA is working with other DHS agencies and DOT operating administrations to develop security standards and initiatives to create a more uniform level of security across all transportation modes without impeding travel or commerce

Civil Aviation Security. First, the flow of intelligence on terrorists, their methods and their plans, has greatly improved our understanding of the threats that we face and helped us focus our resources on meeting those threats. There have been countless times when information shared with airports or airlines has alerted them to threats and encouraged enhanced security on their part.

TSA and the Federal Aviation Administration (FAA) have helped fund many local airport projects to improve perimeter security, such as construction of perimeter access roads, installation of access control systems, electronic surveillance and intrusion detection systems, and security fencing. The realization of and the response to the threat from Man Portable Air Defense Systems (MANPADS) is part of our concern and focus on improved perimeter security, an element of the security plan required for each airport.

One local initiative demonstrates how quickly interagency cooperation can be marshaled to fill security gaps when they are discovered. When perimeter security was breached at New York's JFK Airport, the Port Authority of New York and New Jersey rapidly orchestrated an effective plan to enhance the protection of the remote runways of their facility.[1] A new level of perimeter security is now in place that involves people, technology, and innovation. It is also an example of the products that skilled security planners can develop locally, without an impetus from a Federal agency. Our own TSA security inspectors, FAA's Air Traffic Service, the Port Authority Police, the NYPD Boat Patrol, and the U.S. Coast Guard have joined forces to create a cooperative arrangement that will result in tighter perimeter security including the waterside runways of that airport.

Every passenger entering the sterile areas of an airport is screened by a highly trained force of TSA screeners.[2] Our screeners receive a minimum of 40 hours of classroom training, and 60 hours of on-the-job training. They are subject to periodic proficiency assessments and unannounced training. They are made aware of new threats and methods of concealment. We have also greatly improved the technology used at screening checkpoints and have improved our capability to detect weapons, explosives, and other prohibited items. The combination of our screening force using enhanced technology has resulted in almost 800 arrests at screening checkpoints and the interception of over 4 million prohibited items since the November 19, 2002 deadline to have TSA screeners at all commercial airports. Deploying our screeners at almost 450 commercial airports around the country less than a year after our establishment was a remarkable feat. Similarly, by December 31, 2002, we met the congressional deadline in the Aviation and Transportation Security Act to screen all checked baggage.[3] In large part this was met with explosives detection and explosives trace detection equipment. In some locations during peak periods we screen some bags with a variety of congressionally approved alternative methods.[4]

We expanded the Federal Air Marshal Service (FAMS) from dozens of agents before 9/11 to thousands of highly trained law enforcement officers, flying the skies on high-risk flights. As you know, the FAMs will be transferred to the Bureau of Immigration and Customs Enforcement (BICE). This will create a "surge capacity" to effectively deal with specific threats by cross-training FAMs and BICE agents to help disrupt aviation security threats.

Under FAA rules, all commercial passenger aircraft that fly in the U.S. now have reinforced cockpit doors, making it highly unlikely that terrorists could successfully storm the cockpit.[5] The "Crew Training Common Strategy" (commonly referred to as the "Common Strategy"), was originally developed by FAA to address hijacking threats. It was restructured immediately after 9/11, and TSA and FAA are currently engaged in a further revision to the Common Strategy to address the threats posed by suicide terrorists. Pilots are now trained to not open the flight deck door, and

---

[1] Among the new measures that the Port Authority has instituted are increased perimeter patrols, posting police or security guards in marked patrol cars in unfenced boundary areas during nighttime hours, and directing other mobile patrol units to regularly monitor perimeter activity.

[2] TSA is also operating a pilot program at five airports using private screeners that must meet all TSA eligibility, training, and performance requirements and must receive pay and other benefits equal to those of TSA screeners.

[3] Prior to 9/11, an estimated 5 percent of checked baggage was screened. Now, all checked baggage is screened.

[4] As required by Section 425 of the Homeland Security Act, P.L. 107–296, we are providing the Committee with a classified report every month on our progress on performing electronic screening at all airports by December 31, 2003. As noted in the unclassified segment of the report, we project that at 5 airports it will not be physically possible to provide for electronic screening of all checked baggage by December 31, 2003.

[5] In a widely reported statement, a spokesman for The Boeing Company, which has produced thousands of flight deck door conversion kits, related that the new door withstands bullets and small explosives and can resist a force equivalent to an NFL linebacker hitting it at Olympic sprinter speed.

if terrorists should somehow breach the reinforced flight deck door, they would meet with a flight deck crew determined to protect the flight deck at all costs. An increasing number of pilots are armed and trained to use lethal force against an intruder on the flight deck.

TSA has increased cooperation with our international partners at airports overseas and with air carriers that fly into and out of the United States. We have required thousands of criminal history records checks for U.S. airport workers needing unescorted access to secure areas of the airport and we are working on improving the access process as part of our overall airport security program.

I am proud of the contributions that TSA and its employees have made to our country. It is with great sadness that I report to you that one of our screeners, Sgt. Jaror C. Puello, was recently killed in action while serving in Iraq. Sgt. Puello was a TSA screener at Newark International Airport in New Jersey. Sgt. Puello saved the life of a member of his platoon from a speeding truck but lost his life in the effort. Sgt. Puello leaves behind a wife and three children. Sgt. Puello served this country proudly, in his job with TSA, and in his service to the Army. Many other TSA personnel serve in the Reserves and National Guard and have been called up to active duty.

During the past several months, the media has reported on improvised explosive devices secreted in ordinary items that passengers might carry onto an airplane, continued attempts by terrorists to perfect the shoe bomb apparatus employed, unsuccessfully, by convicted terrorist Richard Reid in December, 2001, and of course the recently reported sting operation concerning an attempt to smuggle a shoulder launched anti-aircraft missile into the United States, although no live missile was involved. These threats are a stark reminder that we must hold our focus on security. The number of prohibited items that TSA screeners continue to intercept from passengers is still large and does not show a downward trend. In May, June, and July of this year the total number of prohibited items that our screeners intercepted increased from 515,792, to 597,310, to 640,891, respectively. The number of intercepted firearms increased from 50, to 67, to 89, but these numbers are down from last year's levels.

Since I last appeared before this Committee I have been able to sign the first Letters of Intent (LOIs) that TSA has issued to airports. These LOIs will provide for the installation of efficient checked baggage systems that are integrated with explosives detection systems, thus reducing unacceptable clutter in the terminal buildings and efficiently moving passengers and checked baggage through the conveyor systems. TSA has established and is applying prioritization criteria to allocate appropriated funds amongst airports through the LOI program. I issued the first series of LOIs to Dallas–Fort Worth International Airport, Boston–Logan International Airport and Seattle–Tacoma International Airport. I awarded another set for McCarran International Airport in Las Vegas, Denver International Airport, and Los Angeles International Airport and Ontario International Airport in California. These six LOIs, covering 7 airports, represent a Federal commitment of approximately $670 million over the next four budget cycles.

We take the threat of MANPADS extremely seriously and continue to perform vulnerability assessments on our airports even as both DHS, through its Science and Technology Directorate, and the Defense Department accelerate their review of technology to find the right way to protect commercial airliners from this threat. Protecting civil aviation from MANPADS remains a multi-faceted undertaking. As noted recently by the Congressional Research Service,[6] effective countermeasures include "improvements or modifications to commercial aircraft, changes to pilot training and air traffic control procedures, and improvements to airport and local security."[7] This includes enhanced perimeter security, particularly if a threat is made known to us via the intelligence information that we receive from a variety of sources. Other components to protect civil aviation from MANPADS are non-proliferation efforts and border and customs enforcement, all key areas that DHS, State Department, the Defense Department, and many other agencies, continue to press forward on. I want to emphasize, however, that there is no credible intelligence that MANPADS are in the hands of terrorists in this country.

We know that we cannot solve all security concerns solely with the power of a strong security workforce. We must be able to develop and deploy new technology to make our screening operations more efficient, less time consuming and costly, and to be able to look beyond the horizon to adapt to new emerging threats. Led

[6] See, *Homeland Security: Protecting Airliners from Terrorist Missiles, Updated March 25, 2003, CRS Report RL31741*

[7] *Id,* at CRS–3

in large part by our Transportation Security Laboratory (TSL), TSA is attempting to do just that.

The certification, purchase, manufacture, and installation of some 1,000 explosives detection systems and 5,300 explosives trace detection machines at more than 400 airports throughout the country in such a short time after TSA was created met an aggressive congressional deadline. Now we are working on faster machines that have a smaller footprint and can find even more minute amounts of explosives. We are improving the efficiency of the current machines even as we move forward with research on the next generation of screening equipment. TSL is looking at new applications of X-ray, electro-magnetic, and nuclear technologies to better probe sealed containers for materials that pose a threat. We are testing two Trace Detection Portals that analyze the air for explosives as passengers pass through them.

I know that this Committee is very interested in blast resistant cargo containers, to hold either cargo or luggage and contain an explosion. The issues we face with devices now available in the marketplace involve weight, cost, and durability. TSA, through TSL, is working on improving this technology for use on wide body aircraft.

In February, I heard the advice of Senator McCain and others loud and clear concerning the importance of good acquisition management and contract oversight. I have initiated a contract oversight strategy that includes significant support from the Defense Contract Management Agency, Defense Contract Audit Agency, and multiple independent third party contractors. TSA has developed a sound investment review process that mirrors the DHS review process. A lot of press has surrounded our contract last year with NCS Pearson, and we will follow the auditor conclusions carefully to ensure we got our money's worth.

Our rightsizing effort continues as we work to find the balance between airport and air carrier needs, and staffing requirements for TSA passenger and baggage screeners. After we ramped up to meet the deadlines for federalizing passenger and baggage screening, we had learned much about our staffing requirements. As we analyzed our staffing model it was clear that there were airports where we had an imbalance in staffing. In some airports this meant we had too many screeners for the passenger load at those locations. At others, particularly those in large metropolitan areas, we had too few screeners. In many locations it became clear that a part-time workforce segment makes sense, given the peaks and valleys of scheduled air carrier service. As a result, and in keeping with our budget limitations, I made a decision to reduce the number of screeners by 3,000 by May 31, 2003, and by an additional 3,000 by September 30th of this year. We have reached these targets. Where we required additional part-time staffing at airports we have opened assessment centers for individuals to apply for these positions.

In light of the fact that TSA met this difficult target of reducing the workforce by 6,000 screeners before the end of this fiscal year, I ask this Committee's understanding of our need to pause and stabilize the screener workforce during the next 3 to 6 months. This will permit TSA to complete the conversion process of many screeners from full-time to part-time status as we reshape the workforce. It will also allow us to complete the immediate requirements to hire additional part-time employees to maintain our current levels of screener workforce and to balance the full-time equivalence (FTE) allocations at the various airports throughout the country.

Cargo security on passenger aircraft remains a matter of concern for this Committee and for all of us engaged in the area of transportation security. I am firmly convinced that our air cargo security strategic plan is on the right track. Proposals to require the physical inspection of every piece of cargo shipped on passenger aircraft without a risk-based targeting strategy are no more practical than similar calls to physically inspect each of the more than 6 million containers that enter the United States each year through our seaports. Proposals of this sort would simply prevent any cargo from being carried onboard passenger aircraft. Rather, we have focused our efforts on three key components in ensuring the security of air cargo.

First, we use a threat-based, risk-management approach. All cargo should be information screened for a determination of the threat and the risk that it poses; moving forward, certain cargo deemed suspicious or high-risk needs to be subjected to heightened security screening under the TSA approach. Part of this process involves banning cargo from unknown shippers, and greatly strengthening the Known Shipper program. Participation in the Known Shipper program is now more rigorous, and all parts of the air cargo supply chain, especially air passenger carriers, all-cargo carriers, and freight forwarders have been given added responsibility for verifying a customer's status in the Known Shipper program. TSA performs inspections of these links in the supply chain to ensure compliance. TSA is also moving forward with the Known Shipper Database and automated Indirect Air Carrier certification/recertification. TSA plans on the full deployment of this database in FY 04.

The second component of our strategic approach to air cargo security involves the use of information analysis to assist in pre-screening cargo. Using information external to TSA, we gather information on whether cargo is of a suspicious origin, warranting additional scrutiny. TSA is already working with BCBP and its National Targeting Center on pre-screening water borne cargo, and will be working closely with BCBP in the development of a similar system for air cargo. Again, we plan to develop and begin deployment of our targeting efforts in FY 04.

The third component in our air cargo security strategic plan involves the development of technology to aid in screening and inspecting air cargo. Our goal is to subject higher-risk shipments to heightened security screening, but TSA will need a toolbox of inspection technologies, as no one technology can be applied in all operating environments. A combination of EDS, ETD, X-ray, canine, and perhaps even some emerging technologies will need to be made available to the field. We will have to overcome a number of hurdles to be able to inspect cargo efficiently by remote means without damaging the contents or unnecessarily delaying shipment. This research and development effort must be supported.

Air cargo security, just like security for all other aspects of the transportation system, is a partnership. The air cargo industry must participate with us in a collaborative effort and must be able to bear its fair share of the costs. I am grateful for the cooperation that TSA has received from the industry through its participation in cargo working groups, an off-shoot of the Aviation Security Advisory Committee. We expect to receive air cargo security recommendations from these working groups in just a few weeks.

Our continuing efforts to improve aviation security inevitably focus on greater information about people who have access to various aspects of the aviation system. That is why our plans to create uniform credentials for workers in the transportation industry are so critical. I am pleased with the continued support that this Committee has given to our Transportation Worker Identification Credential (TWIC) program. TWIC may establish a systemwide credential which, if necessary, has the potential to be used across transportation modes for personnel requiring unescorted physical and/or logical access to secure areas of the transportation system. TWIC will consider multiple access control points to a transportation facility through a variety of transportation vectors. Using funds already appropriated by Congress, we now have a technology evaluation underway at two sites. One is on the East Coast covering the Philadelphia-Delaware River area and the other is on the West Coast in the Los Angeles and Long Beach area. The information that we glean from these technology evaluations will enable us to make key decisions about further development of this program.

Of course, our most visible mission since September 11 has been to keep terrorists off commercial airliners. Our plan to move forward with development, testing, and implementation of the second-generation Computer Assisted Passenger Prescreening System (CAPPS II) is critical to a robust aviation security system. As part of its ongoing dialogue with the public on CAPPS II and related issues, DHS has issued a revised Interim Final Privacy Notice, which provides information regarding CAPPS II, including the type of data that the system will review, and how the data will be used. As always, public comment on the Notice is requested. The closing date for submission of comments is September 30. CAPPS II will be a threat-based system under the direct control of the government and will represent a major improvement over the decentralized, airline-controlled system currently in place. Mr. Chairman, I pledge to continue to work with this Committee to assure you and the Members of this Committee that our development of CAPPS II will enhance security without compromising important privacy rights.

We are also developing the parameters for a pilot program to test key elements of the Registered Traveler program, including background checks, positive identification, and new checkpoint operations. We intend to test these concepts at several airports later this year. Our airline partners have expressed strong interest in working with us.

We have implemented the Federal Flight Deck Officer (FFDO) program. We held the first training class this past April and we trained, deputized, and deployed our first group of volunteer pilots serving as Federal Flight Deck Officers. We closely reevaluated the training, and indeed, the entire program, and we have revamped both. In close cooperation with organizations representing many airline pilots such as the Air Line Pilots Association (ALPA) and the Coalition of Airline Pilots Associations (CAPA), we have begun full-scale training of volunteer pilots. The FFDOs that are currently flying have now flown several thousand flights, quietly providing another layer of security in our system of systems. As more FFDOs are deputized, this number will rise into the tens of thousands of flights.

We will transfer FFDO training on September 8, 2003 from the Federal Law Enforcement Training Center (FLETC) at Glynco, Georgia, to the new permanent site at FLETC's training facility in Artesia, New Mexico. FLETC Glynco was operating over capacity, largely as a result of the added requirements for law enforcement training following September 11. The Artesia facility offers the capability to double the student throughput each week and we plan to do so starting in January 2004. FLETC Artesia is also the home of the basic training program of the FAMS, and thus, has training facilities specifically geared to the unique environment and circumstances present on an aircraft. FLETC Artesia has three environmentally controlled commercial passenger jets on hardstands available for use as tactical training simulators, and ample indoor and outdoor shooting ranges. A delegation of pilots and TSA staff has visited the site and was unanimous in its praise of Artesia as a better option. I intend to use dispersed private sector facilities for the regional semi-annual recertification training required of FFDOs.

TSA's actions to enhance aviation security are not limited to commercial aviation. We have made great strides in the last two years in improving security for the General Aviation (GA) community. This is a substantial undertaking, as there are approximately 220,000 GA aircraft in the United States, responsible for 77 percent of all air traffic, and more than 18,000 landing areas throughout the Nation. In addition to the GA initiatives I reported upon last February, TSA has several other initiatives underway that will continue to improve security in this critical arena. We are working collaboratively with key stakeholders in the GA community to develop and disseminate appropriate security guidelines for the thousands of public and private use GA airports and heliports. TSA is also preparing to launch a GA vulnerability assessment as part of it overall risk management program. We are looking at more in-depth background checks for GA pilots. This would assist in issuing waivers to certain restricted airspace to cleared individuals such as corporate pilots. Finally, we are reviewing some of the restrictions in current Notices to Airmen (NOTAM) to determine their lasting security value. We will engage in appropriate rulemaking to make permanent those restrictions that add real security value.

I want to also bring to your attention the innovative methods we are using to enhance security and provide outstanding customer service. In cooperation with a host of Federal, State, and local agencies, TSA is exploring a variety of methods to smooth the transition of travelers through our transportation system. The first of these intermodal pilot projects, dubbed "Synergy Projects", was initiated in Miami, Florida earlier this year where we have tested integrating the seamless transfer of the baggage of cruise ship passengers from one mode of transportation to another. We have also cooperatively supported a Canadian Government initiative in Vancouver, British Columbia. In conjunction with Royal Caribbean Cruise Lines and Air Canada, this program maintains the security standards of U.S.—U.S. domestic baggage movements. As the success of these initial Synergy Projects becomes better known, other regions of the country are initiating their own proposals to maintain the security of the Nation's transportation system while facilitating the smooth transfer of passengers and their baggage between transportation modes.

As part of the Department's Border and Transportation Directorate, one of our top priorities this year is the development of a comprehensive, coordinated security strategy for the transportation system. To accomplish this, TSA is coordinating the development of a National Transportation System Security Plan (NTSSP). The plan will provide guidance for national-level plans for all transportation modes and will be developed with the collaboration of many partners, including other DHS components such as the Information Analysis and Infrastructure Protection Directorate and the Coast Guard, the Department of Transportation (DOT) modal operating administrations, other Federal Government agencies and private interests. A wide range of perspectives, disciplines, and constituencies will be involved in the Plan's development to ensure the guidance is comprehensive, credible, and executable.

GAO has recommended that DHS and DOT establish a mechanism, such as a memorandum of agreement, to clarify and delineate TSA and DOT roles and responsibilities. We cooperate extensively with DOT and the modal administrations, and value the degree of cooperation that we receive as we work together to secure the transportation systems. We will continue to assess the need for MOAs for the future.

GAO's recommendation for a risk-management approach has been adopted by TSA as a cornerstone for its development of security strategies. Using risk analysis and working under the guidance of the IAIP Directorate, we hope to ascertain the threats, probabilities, and consequences of attacks on the different transportation systems. While security measures will continue to be developed to reflect the many different types of transportation operations, a certain level of consistency must be

established across the systems to ensure that risk is not driven from one mode to another that is perceived less secure.

As they are determined necessary, TSA will develop standards for security that are both cost-effective and non-duplicative. Recognizing that transportation is global in nature, to the greatest extent possible, national standards should be compatible with international standards.

TSA standards will be largely administered and implemented through operating administrations and private sector organizations when practical. Stakeholders will have multiple opportunities to provide input into the development of standards. TSA standards will be performance-based, allowing operators to determine how to best achieve a required level of security. As appropriate, standards will be threat-based and tied to the Homeland Security Alert Level.

Just last week Secretary Ridge announced plans to centralize terrorism and emergency preparedness grant programs within a single office, providing a since point of access for obtaining critical funding. This will ensure that one focal point in the Department is available for potential grantees to tap into the resources and information they need, from applying for funds to protect critical infrastructure to receiving guidance and expertise for first responders. This will allow DHS to provide more consistent grant guidance, coordination, and oversight.

TSA has already distributed substantial funding assistance for maritime and land security projects and will be working closely with other DHS agencies to provide a smooth transition of grant programs under the Secretary's new plan.

For port security assessments and enhancements, TSA issued (under DOT in cooperation with MARAD and the Coast Guard) $92 million in FY 02 funds to 79 grantees for 143 projects. In June 2003, again with the teamwork of the Coast Guard and MARAD, TSA awarded $170 million in FY 03 funds to 199 grantees for 392 projects. TSA is currently completing the selection process for $20 million in port incident response exercise contracts and is beginning the evaluation process for an additional $105 million in port security enhancement grants.

With the assistance of FMCSA and the Federal Transit Administration, TSA selected and recently announced the award of 60 grants for 67 bus security projects totaling $20 million. These grants will enhance driver protection, passenger and baggage screening, and monitoring and communications technologies for over-the-road buses.

Working with DOT and other DHS and Federal agencies, TSA is managing the Operation Safe Commerce (OSC) project. OSC will provide cooperative agreements to identify security weaknesses in the supply chain and fund business-driven pilot projects to enhance container security throughout the supply chain. Utilizing FY 02 and FY 03 funding, TSA awarded funding for 18 projects totaling $58 million to the three largest container load centers in the U.S.—the ports of Los Angeles/Long Beach, Seattle/Tacoma, and New York/New Jersey. Together with the Bureau of Customs and Border Protection, TSA is also co-chairing the Container Working Group, which has recommended potential security technologies and procedures that are being operationally tested in OSC.

To address one of the critical issues in the area of rail hazardous materials security policy, TSA held a workshop to explore the role of placards and their effects on the security of hazardous materials shipments by rail. TSA brought together experts from the response community and railroad community as well as government agencies to discuss security and safety impacts on the treatment of placards for hazardous material shipments by rail.

Last May, GAO's report "Rail Safety and Security—Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed," noted that TSA has not yet developed a risk-based security plan to address rail security. TSA concurs with GAO's recommendation, and is working under the guidance of the IAIP Directorate and with the Department of Transportation to develop a risk-based plan that specifically addresses the security of the Nation's rail infrastructure. This plan will make maximum use of the railroad industry's Terrorism Risk Analysis and Security Management Plan, which is being reviewed consistent with national interests and security goals.

TSA has also provided comments to Amtrak on its Security Investment Plan. Given the vast infrastructure of the passenger rail system, security enhancements should be based on thorough risk assessment and cost-benefit analysis. Close coordination between Amtrak, the Federal Railroad Administration, and TSA is critical as we move forward.

Good intelligence is an important tool for combating terrorism in all modes of transportation. In close coordination with the IAIP Directorate's Intelligence Analysis section, TSA's Transportation Security Intelligence Service (TSIS) receives, assesses, and distributes intelligence related to threats to transportation, and operates

an around-the-clock intelligence watch tied to all national intelligence and law enforcement intelligence programs. It maintains direct connections with TSA's field operations and the security centers of major transportation stakeholders. It tracks intelligence and modal operations developments continuously. Staffed by experienced senior intelligence analysts, the intelligence watch is authorized to alert all appropriate entities to indications of a threat. As part of DHS, TSA is working to integrate its intelligence analysis and products with other intelligence components of DHS while continuing to support its transportation customer base with analysis on transportation security and intelligence.

TSA shares transportation security intelligence directly with the Association of American Railroads (AAR) Operation Center in a manner similar to intelligence sharing for aviation security. To enhance cogent intelligence analysis, industry leaders recently provided briefings on land and maritime transportation to intelligence analysts from the TSIS, the Central Intelligence Agency, the U.S. Coast Guard, DHS's Information Analysis and Infrastructure Protection Directorate, the Northern Command, and the Defense Intelligence Agency through the auspices of TSA. We are also coordinating sponsorship of security clearances and secure communications for security personnel in the transportation industry.

Implementation of the Maritime Transportation Security Act

Leveraging work already undertaken by private industry and within the Federal Government, TSA is collaborating closely with the Coast Guard and the Bureau of Customs and Border Protection to enable DHS to meet the many requirements set forth in the Maritime Transportation Security Act of 2002. For example, in July, the Coast Guard published interim final maritime security regulations to require vessel and facility owners to complete security assessments, develop security plans, and implement security measures and procedures. The regulations will also implement Automatic Identification System (AIS) requirements for certain vessels, as required by MTSA.

These regulations were developed in a collaborative process that involved both TSA and CBP, and are a good example of the benefits of creating the Department of Homeland Security and bringing the Federal Government agencies with complementary missions under one roof. TSA is coordinating with the Coast Guard and the IAIP Directorate to develop a vulnerability assessment tool that may be used by vessel and facility operators to help them meet their obligations under those rules. TSA is also working with the Coast Guard to ensure that the National Maritime Security Plan and the Area Maritime Security Plans are consistent with the National Transportation System Security Plan. TSA will also provide assistance to the Coast Guard and BCBP in conducting foreign port assessments and notifying foreign authorities when ports are not in compliance.

To meet the remaining statutory requirements for which DHS is responsible under MTSA, TSA, BCBP and the Coast Guard are also collaborating closely in the arena of developing performance standards for containerized cargo, secure systems of transportation, and transportation security cards. I am pleased to report that a good portion of the preliminary work necessary to meet these requirements has already been done through the interagency container working group, and programs like Operation Safe Commerce, the Customs Trade Partnership Against Terrorism (C–TPAT), the Container Security Initiative (CSI) and the Transportation Worker Identification Card (TWIC). We are continuing to work closely with BCBP, the Coast Guard, IAIP and other Federal agencies like the Department of Transportation to identify gaps that need to be addressed in these arenas, and will continue to collaborate closely with those partners in identifying how those gaps should be filled.

Conclusion

Analysts can point to a veritable obstacle course of challenges to preparing a comprehensive system of security across the modes. While I recognize and respect the difficulty of meeting these challenges, I am optimistic in that TSA also has many compensating strengths to draw upon. We can look very positively upon the dramatic change in landscape in only two years. We have all learned a great deal very quickly. Also, the enormity of our transportation network and its workers means that we have alert eyes and ears throughout America, along thousands of miles of rail track, at every airport, behind the wheels of trucks and motorcoaches on our highways, throughout our transit stations and systems, and at our ports and loading docks. We also have remarkable, almost instantaneous communications tools to help us reach out as well as share information. Just as important, as this Committee knows so well, the transportation community has decades of success in engineering solutions to national challenges, such as improving transportation safety, building

and maintaining vast transportation systems, and harnessing technology to help them operate more efficiently.

We can only surmount the very real threats to our security by working as a team. You have my assurance that TSA will reach out to all elements of the transportation and security communities, public and private, as we move forward. Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.

Senator HUTCHISON [presiding]. Thank you very much, Admiral Loy.

Mr. Guerrero, welcome.

STATEMENT OF PETER GUERRERO, DIRECTOR, PHYSICAL INFRASTRUCTURE, U.S. GENERAL ACCOUNTING OFFICE; ACCOMPANIED BY GERALD L. DILLINGHAM, DIRECTOR, CIVIL AVIATION ISSUES, AND MARGARET WRIGHTSON, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES

Mr. GUERRERO. Thank you.

Mrs. Hutchison, Mr. Hollings, and Members of the Committee, I appreciate the opportunity to testify today on the security of the Nation's transportation system. With me, to my left, is Gerald Dillingham, and, to his left, Margaret Wrightson, who have both extensive experience in the areas of aviation and port security, respectively. My remarks summarize our statements that we have submitted for the record.

The economic well-being of the United States is critically dependent on the flow of people and goods through the transportation system. The terrorist attacks 2 years ago illustrated the vulnerabilities of that system.

Today, I will discuss the challenges we face in securing the Nation's transportation system, the actions taken by stakeholders to enhance security since September 11, and where we go from here. My comments are based on GAO's work on security issues, including our recent report on transportation security that we prepared for this Committee and several other Members.

Securing the transportation system is fraught with challenges. The first challenge is the sheer size of the transportation system itself. Our transportation infrastructure crisscrosses the Nation and extends beyond our borders to move millions of passengers and tons of freight each day. We have developed a map to illustrate this point. Each of you has before you that map. It's a small posterboard with several overlays attached to it, and we have here, for the audience, a larger board.

The first layer of the map shows the transit systems in metropolitan areas. If you then—that's the white base of the board—and then if you take the first overlay and flip that down for—the second layer shows U.S. ports. The next overlay will show the major airports in this country. The next layer shows the national highway system. The next layer shows large pipelines. And the final layer shows the location of Class I railroads.

When all these layers are put on top of one another, it shows the extreme complexity, extensiveness interconnectivity of the transportation system. It shows how that an incident in one mode of the system can have ripple effects throughout not only the entire system, but also our economy.

The second challenge is funding future security enhancements in an environment where both industry and government are hurting. Throughout our work, transportation stakeholders have repeatedly noted that adequate funding is the most pressing challenge to securing the Nation's transportation system. While some security improvements are relatively inexpensive, such as launching employee awareness campaigns, most require substantial funding. The total cost of enhancing the security over the entire transportation system is unknown. However, given its size, it could amount to hundreds of billions of dollars. The current economic environment makes this a difficult time for private industry, state and local governments, and the Federal Government to make these needed security investments. The sluggish economy has weakened the transportation industry's financial condition by decreasing ridership and revenues. Additionally, many states and the Federal Government are facing very large budget shortfalls.

Every time the national threat level is elevated, transportation stakeholders must provide heightened security. This drains resources from other needs, maintenance is deferred, service expansion plans are put on hold, and employees are diverted from regular duties. While the Federal Government has provided funding for transportation security since September 11, demand has far outstripped amounts made available. Given the high price tag of security enhancements and the limited resources to fund such enhancements, it's critical that government and industry use a risk-management approach to ensure that private and government resources are directed to the highest priorities.

Despite these challenges, numerous actions have been taken to enhance transportation security since September 11. Many transportation operators have conducted security assessments, undertaken emergency drills, and developed plans. State and local governments, which play a critical role in securing the system, because they own a large portion of the transportation network and also because they serve as first responders, have also acted to improve the security of the transportation system.

Numerous agencies at the Federal level have also been involved. Notably, agencies within the Departments of Homeland Security and Transportation have played major efforts in this regard. For example, the Federal Transit Administration in the Department of Transportation has provided grants for emergency drills, security assessments, and training. TSA has met numerous challenges—challenging mandates, really, to aviation security, has hired and deployed an extensive workforce of over 60,000, including passenger and baggage screeners and Federal air marshals. In addition, TSA is working on a number of additional efforts to secure other modes of transportation, such as using a transportation workers identification card program, which would establish a uniform national standard for the secure identification of the 12 million transportation workers.

The Coast Guard, Bureau of Customs and Border and Protection, and the Maritime Administration have also launched a number of initiatives to improve port security and have made important strides in implementing the security provisions of the Maritime Transportation Security Act.

As all of these stakeholders move forward with their security efforts, it will be critically important that their roles and responsibilities are clearly defined and coordinated. Lack of coordination can lead to problems, such as confusion, duplication, and gaps in preparedness. Moreover, lack of coordination can strain intergovernmental relations, drain resources, and raise the potential for problems in responding to acts of terrorism. Therefore, we have recommended that the Department of Homeland Security and the Department of Transportation use a mechanism, such as a memorandum of agreement, to clearly delineate and coordinate their respective roles and responsibilities.

While transportation security has increased since September 11, significant challenges still remain. The remaining work will be challenging and will likely prove as difficult to tackle as the issues addressed over the past 2 years. For example, although securing the aviation system has received considerable attention and funding over the past 2 years, vulnerabilities still remain. These vulnerabilities remain in the areas of airport perimeter, air cargo, and general aviation security, to just cite three examples. Additional strategies to further secure the maritime and land transportation modes, which typically, as we heard today, have open access designed so that they can facilitate commerce and the flow of passengers, must be developed and deployed. As solutions and strategies are developed, their impact on mobility and commerce must also be considered. It will be important to strike the right balance between increasing security and protecting economic vitality and mobility. Meeting these continuing as well as emerging challenges is made more difficult as the Federal Government reorganizes to address these challenges.

The lead player, the Department of Homeland Security, will inevitably encounter funding, human capital, and other organizational challenges typically faced by new organizations, all of which could affect its ability to administer and implement security programs. During this transformation period, coordination among and congressional oversight of key Federal agencies is critical.

In conclusion, securing the transportation system is not an easy or short-term task. Many challenges must be overcome. Transportation stakeholders have worked to strengthen the security of all modes of transportation since September 11. However, much more work remains to be done. It will take a collective and coordinated effort of all transportation stakeholders to meet the continuing challenges and enhance the security of the transportation system. We look forward to working with the Committee in meeting these challenges.

This concludes my prepared statement. We'd be pleased to answer any questions.

[The prepared statements of Mr. Guerrero follows:]

PREPARED STATEMENT OF PETER GUERRERO, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, UNITED STATES GENERAL ACCOUNTING OFFICE

FEDERAL ACTION NEEDED TO ENHANCE SECURITY EFFORTS

Mr. Chairman and Members of the Committee:

We appreciate the opportunity to provide testimony on the security of our Nation's transportation system. Almost 2 years have passed since the attacks of September 11, 2001, demonstrated the vulnerabilities of the Nation's transportation system to the terrorist threat. Although most of the early attention following the September 11 attacks focused on aviation security, emphasis on the other modes of transportation has since grown as concerns are voiced about possible vulnerabilities, such as attempts to introduce weapons of mass destruction into this country through ports or launch chemical attacks on mass transit systems. The entire transportation industry has remained on a heightened state of alert since the attacks.

My testimony today examines (1) challenges in securing the Nation's transportation system; (2) actions transportation operators,[1] as well as state and local governments, have taken since September 11 to enhance security; (3) the Federal role in securing the transportation system and actions the Federal Government has taken to enhance transportation security since September 11; and (4) future actions that are needed to further enhance the security of the Nation's transportation system. My comments are based on our recent report[2] on the security of the transportation system that we prepared for several Members of this Committee as well as a body of our work undertaken since September 11 on homeland security and combating terrorism.[3]

Summary

Transportation stakeholders face numerous challenges in securing the Nation's transportation system. Some of these challenges are common to all modes of transportation; other challenges are specific to aviation, maritime, or land transportation modes. Common security challenges include the extensiveness of the transportation system, the interconnectivity of the system, funding limitations, and the number of stakeholders involved in transportation security. For example, the transportation system includes about 3.9 million miles of roads, over 100,000 miles of rail, almost 600,000 bridges, over 300 ports, 2.2 million miles of pipelines, 500 train stations, and over 5,000 public-use airports. The size of the system simultaneously provides a substantial number of potential targets for terrorists and makes it difficult to secure. Additionally, the number of stakeholders—including over 20 Federal entities, state and local governments, and hundreds of thousands of private businesses—can lead to coordination, communication, and consensus-building challenges. Further exacerbating these challenges are the financial pressures confronting transportation stakeholders. For example, the sluggish economy has weakened the transportation industry's financial condition by decreasing ridership and revenues. The Federal Government has provided additional funding for transportation security since September 11, but demand has far outstripped the additional amounts made available. The aviation, maritime, and land transportation modes also face particular challenges in enhancing security. For instance, maritime and land transportation systems generally have open access designs so that users can enter the systems at multiple points; however, this openness leaves them vulnerable because transportation operators cannot monitor or control who enters or leaves the systems.

---

[1] Transportation operators may be private, public, or quasi-public entities that provide transportation services.

[2] U.S. General Accounting Office, Transportation Security: Federal Action Needed to Help Address Security Challenges, GAO–03–843 (Washington, D.C.: June 30, 2003). For this report, we analyzed the Federal Bureau of Investigation's threat assessment and the administration's security strategies, the Transportation Security Administration (TSA) and the Department of Transportation (DOT) security-related documents and reports, and relevant statutes and regulations. In addition, we interviewed officials from DOT, the National Railroad Passenger Corporation (Amtrak), and TSA as well as representatives from numerous transportation industry associations and transportation security experts. We selected transportation industry and state and local government associations that represent the different modes of transportation and levels of government. We selected transportation security experts on the basis of their knowledge and expertise and reputation as being experts in the transportation security arena. We also consulted with the National Academy of Sciences in identifying appropriate transportation security experts. Finally, we reviewed our past reports on homeland, port, transit, and aviation security and other research on terrorism and transportation security. We conducted our work from February 2003 through May 2003, in accordance with generally accepted government auditing standards.

[3] See Related GAO Products at the end of this testimony.

Despite these challenges, transportation operators and state and local governments have implemented numerous actions to enhance security since September 11. Although security was always a priority, the terrorist attacks elevated the importance and urgency of security. According to representatives from a number of industry associations we interviewed, transportation operators have implemented new security measures or increased the frequency or intensity of existing activities. For example, many transportation operators conducted risk or security assessments, undertook emergency drills, and developed security plans. State and local governments, which play a critical role in securing the system because they own a large portion of the transportation system as well as serve as first responders to incidents involving transportation assets, have also acted to improve the security of the transportation system. Some examples of their actions since September 11 include deploying additional law enforcement personnel and participating in emergency drills with the transportation industry.

The roles of Federal Government agencies in securing the Nation's transportation system are in transition. Prior to September 11, DOT had primary responsibility for the security of the transportation system. In the wake of September 11, Congress created TSA and gave it responsibility for the security of all modes of transportation. During TSA's first year of existence, its primary focus was on aviation security. While TSA was focusing on aviation security, DOT modal administrations [4] launched various initiatives to enhance the security of the maritime and land transportation modes. For example, the Federal Transit Administration (FTA) launched a multipart security initiative to enhance transit security, which included grants for emergency drills, security assessments, and training. TSA has started to assert a greater role in securing the maritime and land transportation modes and is launching a number of new security initiatives. For example, TSA is planning to issue security standards for all modes of transportation. However, a number of representatives from transportation industry and state and local government associations that we contacted expressed concerns about not being adequately involved in TSA's decision-making, such as the development of security standards. DOT modal administrations are also continuing their transportation security efforts. For example, the Federal Highway Administration (FHWA) is coordinating a series of workshops this year on emergency response and preparedness for state departments of transportation and other agencies. The roles and responsibilities of TSA and DOT in transportation security have yet to be clearly delineated, which creates the potential for duplicating and/or conflicting efforts as both entities move forward with their security efforts.

Transportation security experts and representatives from transportation industry and state and local government associations that we spoke with identified a number of actions that they said should be implemented to enhance the security of the Nation's transportation system. In general, they believe that the transportation system is generally more secure today than it was prior to September 11; however, all 1noted that more work is needed to improve the security of the system. Transportation security experts and representatives from transportation industry and state and local government associations identified a number of future actions needed and stated that the identified actions are primarily the responsibility of the Federal Government. For instance, representatives from industry and state and local government associations told us that clarifying Federal roles and coordinating Federal efforts are important because association members are not clear about which agency to contact for their various security concerns and which agency has oversight for certain issues. Some representatives from the transportation industry and state and local government associations also noted that they have received conflicting messages from the different Federal entities.

In our June report, we recommended that the Secretary of Homeland Security and the Secretary of Transportation develop mechanisms, such as a memorandum of agreement, to clearly define the roles and responsibilities of TSA and DOT in transportation security matters.[5] DOT and DHS generally agreed with the report's findings; however, they disagreed with the conclusions and recommendation that their roles and responsibilities in transportation security matters need to be clarified. On the basis of our discussions with transportation security stakeholders, we continue to believe our recommendation would help address transportation security challenges. For example, representatives from several associations stated that their members were unclear as to which agency to contact for their various security con-

[4] DOT's modal administrations are the departmental units responsible for the different modes of transportation, such as the Federal Railroad Administration or the Federal Highway Administration.

[5] GAO–03–843.

cerns and which agency has oversight for certain issues. Furthermore, both DOT and TSA are moving forward with their security efforts, and both entities have statutory responsibilities for transportation security. Therefore, we retained our recommendation that DOT and DHS clarify and delineate their roles and responsibilities in security matters and communicate this information to stakeholders.

Background

The nation's transportation system is a vast, interconnected network of diverse modes. Key modes of transportation include aviation; highways; motor carrier (*i.e.,* trucking); motor coach (*i.e.,* intercity bus); maritime; pipeline; rail (passenger and freight); and transit (*e.g.,* buses, subways, ferry boats, and light rail). The transportation modes work in harmony to facilitate mobility through an extensive network of infrastructure and operators, as well as through the vehicles and vessels that permit passengers and freight to move within the system. For example, the Nation's transportation system moves over 30 million tons of freight and provides approximately 1.1 billion passenger trips each day. The diversity and size of the transportation system make it vital to our economy and national security, including military mobilization and deployment.

Private industry, state and local governments, and the Federal Government all have roles and responsibilities in securing the transportation system. Private industry owns and operates a large share of the transportation system. For example, almost 2,000 pipeline companies and 571 railroad companies own and operate the pipeline and freight railroad systems, respectively. Additionally, 83 passenger air carriers and 640,000 interstate motor coach and motor carrier companies operate in the United States.

State and local governments also own significant portions of the highways, transit systems, and airports in the country. For example, state and local governments own over 90 percent of the total mileage of highways. State and local governments also administer and implement regulations for different sectors of the transportation system and provide protective and emergency response services through various agencies. Although the Federal Government owns a limited share of the transportation system, it issues regulations, establishes policies, provides funding, and/or sets standards for the different modes of transportation. The Federal Government uses a variety of policy tools, including grants, loan guarantees, tax incentives, regulations, and partnerships, to motivate or mandate state and local governments or the private sector to help address security concerns.

Prior to September 11, DOT was the primary Federal entity involved in transportation security matters. However, in response to the attacks on September 11, Congress passed the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and defined its primary responsibility as ensuring security in all modes of transportation.[6] The act also gives TSA regulatory authority over all transportation modes. Since its creation in November 2001, TSA has focused primarily on meeting the aviation security deadlines contained in ATSA. With the passage of the Homeland Security Act on November 25, 2002, TSA, along with over 20 other agencies, was transferred to the new Department of Homeland Security (DHS).[7]

The Transportation System as a Whole Faces Numerous Challenges

The United States maintains the world's largest and most complex national transportation system. Improving the security of such a system is fraught with challenges for both public and private entities. To provide safe transportation for the nation, these entities must overcome issues common to all modes of transportation as well as issues specific to the individual modes of transportation.

All Modes of Transportation Face Common Challenges

Although each mode of transportation is unique, they all face some common challenges in trying to enhance security. Common challenges stem from the extensiveness of the transportation system, the interconnectivity of the system, funding security improvements, and the number of stakeholders involved in transportation security.

Size and Diversity of Transportation Modes Create Security Challenges

The size of the transportation system makes it difficult to adequately secure. The transportation system's extensive infrastructure crisscrosses the Nation and extends beyond our borders to move millions of passengers and tons of freight each day. The extensiveness of the infrastructure as well as the sheer volume of freight and pas-

[6] P.L. No. 107–71, 115 Stat. 597 (2001).
[7] P.L. No. 107–296, 116 Stat. 2135 (2002).

sengers moved through the system creates an infinite number of targets for terrorists. Furthermore, as industry representatives and transportation security experts repeatedly noted, the extensiveness of the infrastructure makes equal protection for all assets impossible.

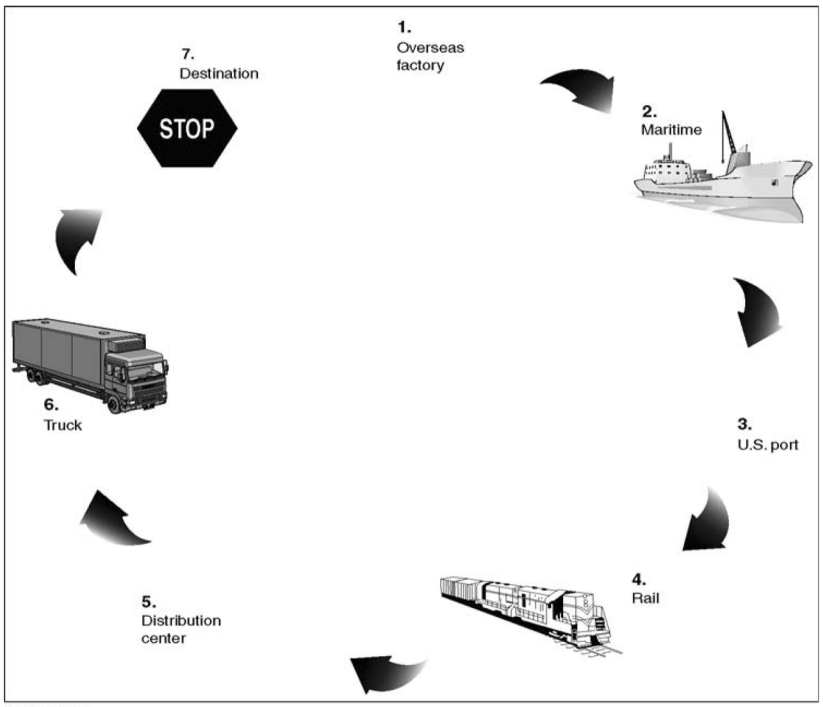
Protecting transportation assets from attack is made more difficult because of the tremendous variety of transportation operators. Some are multibillion-dollar enterprises, and others have very limited facilities and very little traffic. Some are public agencies, such as state departments of transportation, and some are private businesses. Some transportation operators carry passengers, and others haul freight. Additionally, the type of freight moved through the different modes is similarly varied. For example, the maritime, motor carrier, and rail operators haul freight as diverse as dry bulk (grain) and hazardous materials.

Interconnectivity and Interdependency Also Present Challenges

Additional challenges are created by the interconnectivity and interdependency among the transportation modes and between the transportation sector and nearly every other sector of the economy. The transportation system is interconnected or intermodal because passengers and freight can use multiple modes of transportation to reach a destination. For example, from its point of origin to its destination, a piece of freight, such as a shipping container, can move from ship to train to truck. (See fig. 1.) The interconnective nature of the transportation system creates several security challenges. First, the effects of events directed at one mode of transportation can ripple throughout the entire system. For example, when the port workers in California, Oregon, and Washington went on strike in 2002, the railroads saw their intermodal traffic decline by almost 30 percent during the first week of the strike, compared with the year before. Second, the interconnecting modes can contaminate each other—that is, if a particular mode experiences a security breach, the breach could affect other modes.[8] An example of this would be if a shipping container that held a weapon of mass destruction arrived at a U.S. port where it was placed on a truck or train. In this case, although the original security breach occurred in the port, the rail or trucking industry would be affected as well. Thus, even if operators within one mode established high levels of security they could be affected because of the security efforts, or lack thereof, of the other modes. Third, intermodal facilities where a number of modes connect and interact—such as ports—are potential targets for attack because of the presence of passengers, freight, employees, and equipment at these facilities.

[8] Similarly, there are opportunities for cross contamination within the same mode. For example, a bag containing an explosive device could be placed on one airline and then transferred to another airline where it explodes.

Figure 1: Illustration of Possible Freight Movements within the Transportation System



Source: GAO.

Interdependencies also exist between transportation and nearly every other sector of the economy. Consequently, an event that affects the transportation sector can have serious impacts on other industries. For example, when the war in Afghanistan began in October 2001, the rail industry restricted the movement of many hazardous materials, including chlorine, because of a heightened threat of a terrorist attack. However, within days, many major water treatment facilities reported that they were running out of chlorine, which they use to treat drinking water, and would have to shut down operations if chlorine deliveries were not immediately resumed.

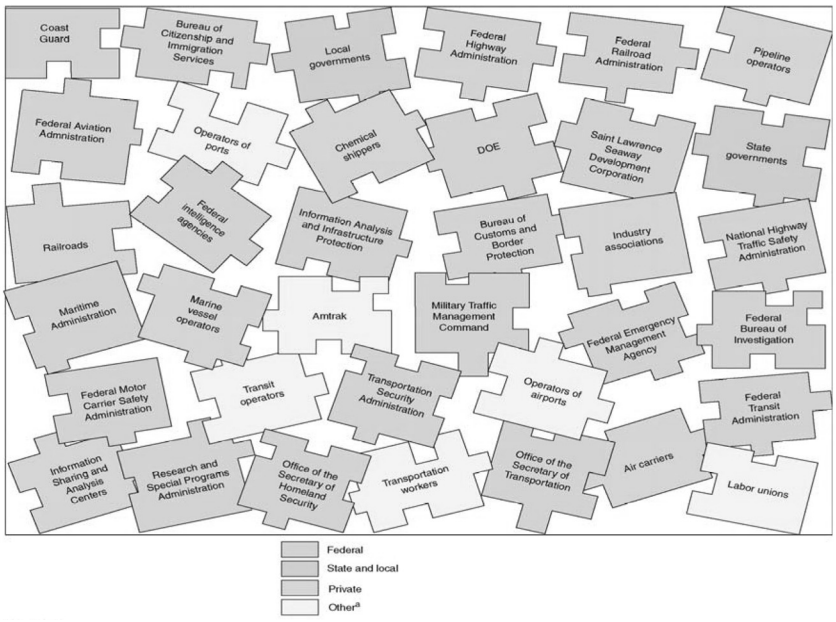
The Number of Stakeholders Creates Challenges

Securing the transportation system is made more difficult because of the number of stakeholders involved. As illustrated in figure 2, numerous entities at the federal, state, and local levels, including over 20 Federal entities and thousands of private sector businesses, play a key role in transportation security. For example, the Departments of Energy, Transportation, and Homeland Security; state governments; and about 2,000 pipeline operators are all responsible for securing the pipeline system. The number of stakeholders involved in transportation security can lead to communication challenges, duplication, and conflicting guidance. Representatives from several state and local government and industry associations told us that their members are receiving different messages from the various Federal agencies involved in transportation security. For instance, one industry representative noted that both TSA and DOT asked the industry to implement additional security measures when the Nation's threat condition was elevated to orange at the beginning of the Iraq War;[9] however, TSA and DOT were not consistent in what they wanted

[9] DHS created the Homeland Security Advisory System. The system has five threat conditions—ranging from low to severe—representing different levels of risk for terrorist attacks.

done—that is, they were asking for different security measures. Moreover, many representatives commented that the Federal Government needs to better coordinate its security efforts. These representatives noted that dealing with multiple agencies on the same issues and topics is frustrating and time consuming for the transportation sector.

Figure 2: Key Stakeholders in Transportation Security



Source. GAO.
[a] "Other" includes private, public, or quasi-public entities.

The number of stakeholders also makes it difficult to achieve the needed cooperation and consensus to move forward with security efforts. As we have noted in past reports, coordination and consensus-building are critical to successful implementation of security efforts. Transportation stakeholders can have inconsistent goals or interests, which can make consensus-building challenging. For example, from a safety perspective, vehicles that carry hazardous materials should be required to have placards that identify the contents of a vehicle so that emergency personnel know how best to respond to an incident. However, from a security perspective, identifying placards on vehicles that carry hazardous materials make them a potential target for attack.

Funding Is Key Challenge

According to transportation security experts and state and local government and industry representatives we contacted, funding is the most pressing challenge to securing the Nation's transportation system. Although some security improvements are inexpensive, such as removing trash cans from subway platforms, most require substantial funding. Additionally, given the large number of assets to protect, the sum of even relatively less expensive investments can be cost prohibitive. For example, reinforcing shipping containers to make them more blast resistant is one way to improve security, which would cost about $15,000 per container. With several million shipping containers in use, however, this tactic would cost billions of dollars if all of them were reinforced. The total cost of enhancing the security of the entire transportation system is unknown; however, given the size of the system, it could amount to tens of billions of dollars.

The current economic environment makes this a difficult time for private industry or state and local governments to make security investments. According to industry representatives and experts we contacted, most of the transportation industry operates on a very thin profit margin, making it difficult for the industry to pay for addi-

tional security measures. The sluggish economy has further weakened the transportation industry's financial condition by decreasing ridership and revenues. For example, airlines are in the worst fiscal crisis in their history, and several have filed for bankruptcy. Similarly, the motor coach and motor carrier industries and Amtrak report decreased revenues because of the slow economy. In addition, nearly every state and local government is facing a large budget deficit for Fiscal Year 2004. For example, the National Governors Association estimates that states are facing a total budget shortfall of $80 billion for Fiscal Year 2004. Given the tight budget environment, state and local governments and transportation operators must make difficult trade-offs between transportation security investments and other needs, such as service expansion and equipment upgrades. According to the National Association of Counties, many local governments are planning to defer some maintenance of their transportation infrastructure to pay for some security enhancements.

Further exacerbating the problem of funding security improvements is the additional costs the transportation sector incurs when the Federal Government elevates the national threat condition. Industry representatives stated that operators tighten security, such as increasing security patrols, when the national threat condition is raised or intelligence information suggests an increased threat against their mode. However, these representatives stated that these additional measures drain resources and are not sustainable. For example, Amtrak estimates that it spends an additional $500,000 per month for police overtime when the national threat condition is increased. Transportation industry representatives also noted that employees are diverted from their regular duties to implement additional security measures, such as guarding entranceways, in times of increased security, which hurts productivity.

The Federal Government has provided additional funding for transportation security since September 11, but demand has far outstripped the additional amounts made available. For example, Congress appropriated a total of $241 million for grants for ports, motor carriers, and Operation Safe Commerce in 2002.[10] However, as table 1 shows, the grant applications TSA has received for these security grants totaled $1.8 billion—nearly 8 times more than the amount available. Due to the costs of security enhancements and the transportation industries' and state and local governments' tight budget environments, the Federal Government is likely to be viewed as a source of funding for at least some of these enhancements. However, given the constraints on the Federal budget as well as competing claims for Federal assistance, requests for Federal funding for transportation security enhancements will likely continue to exceed available resources.

Table 1.—Comparison of Selected Transportation Security Grant Requests with Federal Funding Available, 2002 to 2003

[Dollars in millions]

Type of grant	Amount appropriated	Total amount requested in all grant applications
Port security grants [a]	$93.3	$697
Port security grants [b]	105	996
Intercity bus grants [b]	15	45.6
Operation Safe Commerce grants [b]	28	97.9
Total	$241.3	$1,836.5

Source: TSA.
Note: Both the Department of Defense and Emergency Supplemental Appropriations Act (P.L. No. 107–117) and the Supplemental Appropriations Act (P.L. No. 107–206) provided funding for port security grants.
[a] P.L. No. 107–117, 115 Stat. 2230 (2002).
[b] P.L. No. 107–206, 116 Stat. 820 (2002).

Balancing Potential Economic Impacts and Security Enhancements Is Also Challenging

Another challenge is balancing the potential economic impacts of security enhancements with the benefits of such measures. Although there is broad support for greater security, this task is a difficult one because the Nation relies heavily on a free and expeditious flow of goods. Particularly with "just-in-time" deliveries, which require a smooth and expeditious flow through the transportation system, delays or

[10] Operation Safe Commerce focuses on using new technology, such as container seals, to help shippers ensure the integrity of the cargo included in containers being sent to the United States.

disruptions in the supply chain could have serious economic impacts. As the Coast Guard Commandant stated about the flow of goods through ports, "even slowing the flow long enough to inspect either all or a statistically significant random selection of imports would be economically intolerable." [11]

Furthermore, security measures may have economic and competitive ramifications for individual modes of transportation. For instance, if the Federal Government imposed a particular security requirement on the rail industry and not on the motor carrier industry, the rail industry might incur additional costs and/or lose customers to the motor carrier industry. Striking the right balance between increasing security and protecting the economic vitality of the national economy and individual modes will remain an important and difficult task.

Individual Transportation Modes Also Confront Unique Challenges

In addition to the overarching challenges that transportation stakeholders will face in attempting to improve transportation security, they also face a number of challenges specific to the aviation, maritime, and land transportation modes. Although aviation security has received a significant amount of attention and funding since September 11, more work is needed. In general, transportation security experts believe that the aviation system is more secure today than it was prior to September 11. However, aviation experts and TSA officials noted that significant vulnerabilities remain. For example:

- Perimeter security: Terrorists could launch attacks, such as launching shoulder-fired missiles, from a location just outside an airport's perimeter. Since September 11, airport operators have increased their patrols of airport perimeter areas, but industry officials state that they do not have enough resources to completely protect against these attacks.
- Air cargo security: Although TSA has focused much effort and funding on ensuring that bombs and other threat items are not carried onto planes by passengers or in their luggage, vulnerabilities exist in securing the cargo carried aboard commercial passenger and all-cargo aircraft. For example, employees of shippers and freight forwarders are not universally subject to background checks. Theft is also a major problem in air cargo shipping, signifying that unauthorized personnel may still be gaining access to air cargo shipments. Air cargo shipments pass through several hands in going from sender to recipient, making it challenging to implement a system that provides adequate security for air cargo. According to TSA officials, TSA is developing a strategic plan to address air cargo security and has undertaken a comprehensive outreach process to strengthen security programs across the industry.
- General aviation security: Although TSA has taken several actions related to general aviation [12] since September 11, this segment of the industry remains potentially more vulnerable than commercial aviation. For example, general aviation pilots are not screened prior to taking off, and the contents of a plane are not examined at any point. According to TSA, solutions that can be implemented relatively easily at the Nation's commercial airports are not practical at the 19,000 general aviation airports. It would be very difficult to prevent a general aviation pilot intent on committing a terrorist attack with his or her aircraft from doing so. The vulnerability of the system was illustrated in January 2002, when a teenage flight student from Florida crashed his single-engine airplane into a Tampa skyscraper. TSA is working with the appropriate stakeholders to close potential security gaps and to raise the security standards across this diverse segment of the aviation industry.

Maritime and land transportation systems have their own unique security vulnerabilities. For example, maritime and land transportation systems generally have an open design, meaning the users can access the system at multiple points. The systems are open by design so that they are accessible and convenient for users. In contrast, the aviation system is housed in closed and controlled locations with few entry points. The openness of the maritime and land transportation systems can leave them vulnerable because transportation operators cannot monitor or control who enters or leaves the systems. However, adding security measures that restrict the flow of passengers or freight through the systems could have serious consequences for commerce and the public.

---

[11] Meeting the Homeland Security Challenge: A Principled Strategy for a Balanced and Practical Response (September 2001); and Global Trade: America's Achilles' Heel (February 2002) by Admiral James M. Loy and Captain Robert G. Ross, U.S. Coast Guard.

[12] General aviation includes more than 200,000 corporate and privately owned aircraft at over 19,000 airports.

Individual maritime and land transportation modes also have unique challenges and vulnerabilities. For example, representatives from the motor carrier industry noted that the high turnover rate (about 40 to 60 percent) of drivers means that motor carrier operators must be continually conducting background checks on new drivers, which is expensive and time consuming. Additionally, as we noted in our report on rail safety and security,[13] the temporary storage of hazardous materials in unsecured or unmonitored rail cars while awaiting delivery to their ultimate destinations is a potential vulnerability. Specifically, unmonitored chemical cars could develop undetected leaks that could threaten the nearby population and environment. In addition, representatives from the motor coach industry commented that the number of used motor coaches on the market, coupled with the lack of guidance or requirements on buying or selling these vehicles, is a serious vulnerability. In particular, there are approximately 5,000 used motor coaches on the market; however, there is very little information on who is selling and buying them, nor is there any consistency among motor coach operators in whether they remove their logos from the vehicles before they are sold. These vehicles could be used as weapons or to transport weapons. Federal Motor Carrier Safety Administration officials told us they have not issued guidance to the industry on this potential vulnerability because TSA is responsible for security and therefore would be responsible for issuing such guidance.

Transportation Operators and State and Local Governments Have Taken Steps to Improve Security

Since September 11, transportation operators and state and local governments have been working to strengthen security, according to associations we contacted. Although security was a priority before September 11, the terrorist attacks elevated the importance and urgency of transportation security for transportation operators and state and local governments. According to representatives from a number of industry associations we interviewed, transportation operators have implemented new security measures or increased the frequency or intensity of existing activities. Some of the most common measures cited include conducting vulnerability or risk assessments, tightening access control, intensifying security presence, increasing emergency drills, developing or revising security plans, and providing additional training. (Figure 3 is a photograph from an annual emergency drill conducted by the Washington Metropolitan Area Transit Authority.)

Figure 3: Emergency Drill in Progress

At a planned emergency drill, firefighters practice rescuing passengers from a Washington Metropolitan Area Transit Authority subway car.

Source: GAO.

[13] U.S. General Accounting Office, Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed, GAO–03–435 (Washington, D.C.: Apr. 30, 2003).

As we have previously reported, state and local governments are critical stakeholders in the Nation's homeland security efforts. This is equally true in securing the Nation's transportation system. State and local governments play a critical role, in part, because they own a significant portion of the transportation infrastructure, such as airports, transit systems, highways, and ports. For example, state and local governments own over 90 percent of the total mileage of the highway system. Even when state and local governments are not the owners or operators, they nonetheless are directly affected by the transportation modes that run through their jurisdictions. Consequently, the responsibility for protecting this infrastructure and responding to emergencies involving the transportation infrastructure often falls on state and local governments.

Security efforts of local and state governments have included developing counter terrorist plans, participating in training and security-related research, participating in transportation operators' emergency drills and table-top exercises, conducting vulnerability assessments of transportation assets, and participating in emergency planning sessions with transportation operators. Some state and local governments have also hired additional law enforcement personnel to patrol transportation assets. Much of the funding for these efforts has been covered by the state and local governments, with a bulk of the expenses going to personnel costs, such as for additional law enforcement officers and overtime.

Congress and Federal Agencies Have Taken Numerous Actions to Enhance Security, but Roles Remain Unclear

Congress, DOT, TSA, and other Federal agencies have taken numerous steps to enhance transportation security since September 11. The roles of the Federal agencies in securing the Nation's transportation system, however, are in transition. Prior to September 11, DOT had primary responsibility for the security of the transportation system. In the wake of September 11, Congress created TSA and gave it responsibility for the security of all modes of transportation. However, DOT and TSA have not yet formally defined their roles and responsibilities in securing all modes of transportation. Furthermore, TSA is moving forward with plans to enhance transportation security. For example, TSA plans to issue security standards for all modes. DOT modal administrations are also continuing their security efforts for different modes of transportation.

Congress and Federal Agencies Have Acted to Enhance Transportation Security

Congress has acted to enhance the security of the Nation's transportation system since September 11. In addition to passing the Aviation and Transportation Security Act (ATSA),[14] Congress passed a number of other key pieces of legislation aimed at improving transportation security. For example, Congress passed the USA PATRIOT Act of 2001,[15] which mandates Federal background checks of individuals operating vehicles carrying hazardous materials; and the Homeland Security Act,[16] which created DHS and moved TSA to the new department.[17] Congress also provided funding for transportation security enhancements through various appropriations acts. For example, the 2002 Supplemental Appropriations Act, in part, provided (1) $738 million for the installation of explosives detection systems in commercial service airports, (2) $125 million for port security activities, and (3) $15 million to enhance the security of intercity bus operations.

Federal agencies, notably TSA and DOT, have also taken steps to enhance transportation security since September 11. In its first year of existence, TSA worked to establish its organization and focused primarily on meeting the aviation security deadlines contained in ATSA. In January 2002, TSA had 13 employees to tackle securing the Nation's transportation system; 1 year later, TSA had about 65,000 employees. TSA reports that it met over 30 deadlines during 2002 to improve aviation security, including two of its most significant deadlines—to deploy Federal passenger screeners at airports across the Nation by November 19, 2002; and to screen every piece of checked baggage for explosives by December 31, 2002.[18] According to

---

[14] P.L. No. 107–71, 115 Stat. 597 (2001).

[15] P.L. No. 107–56, 115 Stat. 272 (2001).

[16] P.L. No. 107–296, 116 Stat. 2135 (2002).

[17] The U.S. Coast Guard was also transferred to DHS. In the Terms of Reference Regarding the Respective Roles of the U.S. Coast Guard and the Transportation Security Administration, the Coast Guard is designated as the lead DHS agency for maritime security and is directed to coordinate as appropriate with other agencies. The document further notes that a supporting memorandum of agreement between the Commandant of the Coast Guard and the Administrator of the Transportation Security Administration is being developed.

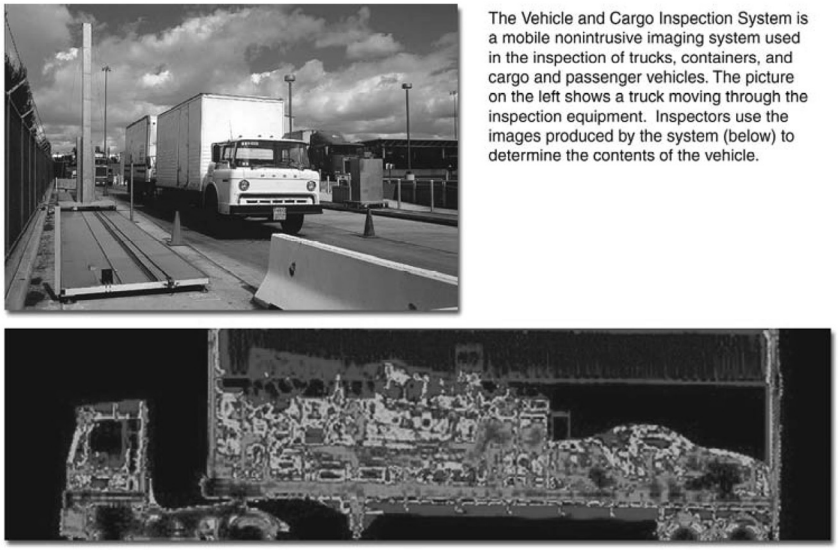
[18] The Homeland Security Act, P.L. 107–296 (November 25, 2002) the legislation that created DHS, amended this deadline to allow some airports up to an extra year (December 31, 2003)

TSA, other completed TSA activities included recruiting, hiring, training, and deploying about 56,000 Federal screeners; awarding grants for port security; and implementing performance management system and strategic planning activities to create a results-oriented culture.

As TSA worked to establish itself and improve the security of the aviation system, DOT modal administrations acted to enhance the security of air, land, and maritime transportation. (See app. I for a table listing the actions taken by DOT modal administrations since September 11.) The actions taken by the DOT modal administrations have varied. For example, FTA launched a multipart initiative for mass transit agencies that provided grants for emergency drills, offered free security training, conducted security assessments at 36 transit agencies, provided technical assistance, and invested in research and development. The Federal Motor Carrier Safety Administration developed three courses for motor coach drivers. The responses of the various DOT modal agencies have varied due to differences in authority and resource limitations.

In addition to TSA and DOT modal administrations, other Federal agencies have also taken actions to improve security. For example, the Bureau of Customs and Border Protection (CBP), previously known as the U.S. Customs Service, has launched a number of initiatives aimed at strengthening the security of the U.S. border.[19] Some of the specific security initiatives that CBP has implemented include establishing the Customs Trade Partnership Against Terrorism (C–TPAT), which is a joint government business initiative aimed at securing the supply chain of global trade against terrorist exploitation; and launching the Container Security Initiative (CSI), which is designed specifically to secure ocean-going sea containers. In addition, CBP has developed and/or deployed tools to detect weapons of mass destruction in cargo containers and vehicles, such as the new mobile gamma ray imaging devices pictured in figure 4.

Figure 4: Photograph of Inspection Equipment in Use



The Vehicle and Cargo Inspection System is a mobile nonintrusive imaging system used in the inspection of trucks, containers, and cargo and passenger vehicles. The picture on the left shows a truck moving through the inspection equipment. Inspectors use the images produced by the system (below) to determine the contents of the vehicle.

Source: Science Applications International Corporation (SAIC) ©2003.

---

to deploy all of the necessary explosive detection equipment to enable TSA to screen all checked baggage. TSA reported that as of December 31, 2002, about 90 percent of all checked baggage were screened with an explosive detection system or explosives trace detection equipment and the remaining checked baggage was screened using alternative means as is allowed under the law.

[19] The U.S. Customs Service was transferred from the Department of Treasury to DHS in the Homeland Security Act of 2002 (P.L. No. 107–296, 116 Stat. 2135 (2002)) and renamed the Bureau of Customs and Border Protection.

TSA Moves Forward as its Role in Transportation Security Evolves

TSA is moving forward with efforts to secure the entire transportation system. TSA has adopted a systems approach—that is, a holistic rather than a modal approach—to securing the transportation system. In addition, TSA is using risk management principles to guide its decision-making. TSA is also planning to establish security standards for all modes of transportation and is launching a number of new security efforts for the maritime and land transportation modes.

TSA Adopts a Systems Approach and Risk Management Principles

Using the systems approach, TSA plans to address the security of the entire transportation system as a whole, rather than focusing on individual modes of transportation. According to TSA officials, using a systems approach to security is appropriate for several reasons. First, the transportation system is intermodal, interdependent, and international. Given the intermodalism of the system, incidents in one mode of transportation could affect other modes. Second, it is important not to drive terrorism from one mode of transportation to another mode because of perceived lesser security—that is, make a mode of transportation a more attractive target because another mode is "hardened" with additional security measures. Third, it is important that security measures for one mode of transportation are not overly stringent or too economically challenging compared with the measures used for other modes. Fourth, it is important that the attention on one aspect of transportation security (*e.g.,* cargo, infrastructure, or passengers) does not leave the other aspects vulnerable.

TSA has also adopted a risk management approach for its efforts to enhance the security of the Nation's transportation system. A risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions in order to link resources with prioritized efforts. (See app. II for a description of the key elements of a risk management approach.) The highest priorities emerge where the three elements of risk management overlap. For example, transportation infrastructure that is determined to be a critical asset, vulnerable to attack, and a likely target would be most at risk and therefore would be a higher priority for funding compared with infrastructure that was only vulnerable to attack. According to TSA officials, risk management principles will drive all decisions—from standard-setting to funding priorities to staffing.

Using risk management principles to guide decision-making is a good strategy, given the difficult trade-offs TSA will likely have to make as it moves forward with its security efforts. We have advocated using a risk management approach to guide Federal programs and responses to better prepare against terrorism and other threats and to better direct finite national resources to areas of highest priority. As representatives from local government and industry associations and transportation security experts repeatedly noted, the size of the transportation system precludes equal protection for all assets; moreover, the risks vary by transportation assets within modes and by modes. In addition, requests for funding for transportation security enhancements will likely exceed available resources. Risk management principles can help TSA determine security priorities and identify appropriate solutions.

TSA Plans to Issue National Security Standards

TSA plans to issue national security standards for all modes of transportation. The Federal Government has historically set security standards for the aviation sector. For instance, prior to the passage of ATSA, FAA set security standards that the airlines were required to follow in several areas including, screening equipment, screener qualifications, and access control systems. In contrast, prior to the September 11 attacks, limited statutory authority existed to require measures to ensure the security of the maritime and land transportation systems. According to a TSA report, the existing regulatory framework leaves the maritime and land transportation systems unacceptably vulnerable to terrorist attack. For example, the rail, transit, and motor coach transportation systems are subject to no mandatory security requirements, resulting in little or no screening of passengers, baggage, or crew. Additionally, seaborne passenger vessel and seaport terminal operators have inconsistent levels and methods of screening and are largely free to set their own rules about the hiring and training of security personnel. Hence, TSA will set standards to ensure consistency among modes and across the transportation system and to reduce the transportation system's vulnerability to attacks.[20]

[20] The Information Analysis and Infrastructure Protection Directorate within DHS is working with TSA, the Coast Guard, and other Federal agencies on developing a set of national stand-

According to TSA officials and documents, TSA's standards will be performance-, risk-, and threat-based and may be mandatory. More specifically:

- *Standards will be performance-based.* Rather than being prescriptive standards, TSA standards will be performance-based, which will allow transportation operators to determine how best to achieve the desired level of security. TSA officials believe that performance-based standards provide for operator flexibility, allow operators to use their professional judgment in enhancing security, and encourage technology advancement.
- *Standards will be risk-based.* Standards will be set for areas for which assessments of the threats, vulnerabilities, and criticality indicate that an attack would have a national impact. A number of factors could be considered in determining "national impact," such as fatalities and economic damage.
- *Standards will be threat-based.* The standards will be tied to the national threat condition and/or local threats. As the threat condition escalates, the standards will require transportation operators to implement additional countermeasures.
- *Standards may be mandatory.* The standards will be mandatory when the risk level is too high or unacceptable. TSA officials stated that in these cases, mandatory standards are needed to ensure accountability. In addition, according to TSA officials, voluntary requirements put security-conscious transportation operators that implement security measures at a competitive disadvantage—that is, they have spent money that their competitors may not have spent. This creates a disincentive for transportation operators to implement voluntary requirements. TSA officials believe that mandatory standards will reduce this problem. In determining whether mandatory standards are needed, TSA will review the results of criticality and vulnerability assessments, current best practices, and voluntary compliance opportunities in conjunction with the private sector and other government agencies.

Although TSA officials expect some level of resistance to the standards by the transportation industry, they believe that their approach of using risk-, threat-, and performance-based standards will increase the acceptance of the standards. For example, performance-based standards allow for more operator flexibility in implementing the standards, compared with rigid, prescriptive standards. Moreover, TSA plans to issue only a limited number of standards—that is, standards will be issued only when assessments of the threats, vulnerabilities, and criticality indicate that the level of risk is too high or unacceptable.

TSA also expects some level of resistance to the standards from DOT modal administrations. Although TSA will establish the security standards, TSA expects that they will be administered and implemented by existing agencies and organizations. DOT modal administrations may be reluctant to assume this role because doing so could alter their relationships with the industry. Historically, the missions of DOT surface transportation modal administrations have largely focused on maintaining operations and improving service and safety, not regulating security. Moreover, the authority to regulate security varies by DOT modal administration. For example, FTA has limited authority to regulate and oversee security at transit agencies. In contrast, FRA has regulatory authority for rail security, and DOT's Office of Pipeline Safety has responsibility for writing safety and security regulations for liquefied natural gas storage facilities. In addition, DOT modal administrations may be reluctant to administer and implement standards because of resource concerns. FHWA officials commented that given the current uncertainty about the standards and their impacts, FHWA is reluctant to commit, in advance, staff or funding to enforce new security standards.

Gaining Stakeholder Buy-in is Critical for Standards to Work, but Stakeholders Express Concerns

Because transportation stakeholders will be involved in administering, implementing, and/or enforcing TSA standards, stakeholder buy-in is critical to the suc-

---

ards that would apply to all ports. These efforts are well under way. The Coast Guard has been developing a set of standards since May 2002 as part of its efforts to conduct vulnerability assessments for all U.S. ports. The standards will go into effect on July 1, 2004, as part of the International Convention for the Safety of Life at Sea (SOLAS) amendments and the International Ship and Port Facility Security Code (ISPS) that was adopted by the International Maritime Organization conference in December 2002. The Coast Guard considers that the implementation of these standards is best done through mandating compliance with the SOLAS amendments and the ISPS Code. According to TSA, because of the Coast Guard's significant role in securing maritime transportation, TSA will likely play a coordination role in the maritime arena.

cess of this initiative. Compromise and consensus on the part of stakeholders are also necessary. However, achieving such consensus and compromise may be difficult, given the conflicts between some stakeholders' goals and interests.

Transportation stakeholders we contacted also expressed a number of concerns about TSA's plan to issue security standards for all modes of transportation. For example, industry associations expressed concerns that the standards would come in the form of unfunded mandates—that is, the Federal Government would not provide funding to implement mandatory standards. According to the industry and state and local government associations we spoke to, unfunded mandates create additional financial burdens for transportation operators, who are already experiencing financial difficulties. Industry representatives also expressed concern that TSA has not adequately included the transportation industry in its development of standards. Many industry representatives and some DOT officials we met with were unsure of whether TSA was issuing standards, what the standards would entail, or the time frames for issuing the standards. The uncertainty about the pending standards can lead to confusion and/or inaction. For example, Amtrak officials noted that they are reluctant to spend money to implement certain security measures because they are worried that TSA will subsequently issue standards that will require Amtrak to redo its efforts. Transportation stakeholders also raised other concerns about TSA's plans to issues standards, including questioning whether TSA has the necessary expertise to develop appropriate standards and whether mandatory standards, as opposed to voluntary standards, are prudent.

TSA Is Launching Other Security Initiatives

TSA is also working on a number of additional security efforts, such as establishing the Transportation Workers Identification Card (TWIC) program; developing the next generation of the Computer Assisted Passenger Pre-Screening System; developing a national transportation system security plan; and exploring methods to integrate operations and security, among other things. The TWIC program is intended to improve access control for the 12 million transportation workers who require unescorted physical or cyber access to secure areas of the Nation's transportation modes by establishing a uniform, nationwide standard for secure identification of transportation workers. Specifically, TWIC will combine standard background checks and biometrics so that a worker can be positively matched to his/her credential. Once the program is fully operational, the TWIC would be the standard credential for transportation workers and would be accepted by all modes of transportation. According to TSA, developing a uniform, nationwide standard for identification will minimize redundant credentialing and background checks.

DOT Modal Agencies Are Continuing Forward with Their Security Efforts

As TSA moves forward with new security initiatives, DOT modal administrations are also continuing their security efforts and, in some cases, launching new security initiatives. For example, FHWA is coordinating a series of workshops this year on emergency response and preparedness for state departments of transportation and other agencies. FTA also has a number of initiatives currently under way in the areas of public awareness, research, training, technical assistance, and intelligence sharing. For example, FTA developed a list of the top 20 security actions transit agencies should implement and is currently working with transit agencies to assist them in implementing these measures.

FAA is also continuing its efforts to enhance cyber security in the aviation system. Although the primary responsibility for securing the aviation system was transferred to TSA, FAA remains responsible for protecting the Nation's air traffic control system—both the physical security of its air traffic control facilities and computer systems. The air traffic control system's computers help the Nation's air traffic controllers to safely direct and separate traffic—sabotaging this system could have disastrous consequences. FAA is moving forward with efforts to increase the physical security of its air traffic control facilities and ensure that contractors who have access to the air traffic control system undergo background checks.

TSA's and DOT's Roles and Responsibilities Have Not Been Clearly Defined

The roles and responsibilities of TSA and DOT in transportation security have yet to be clearly delineated, which creates the potential for duplicating or conflicting efforts as both entities move forward with their security efforts. DOT modal administrations were primarily responsible for the security of the transportation system prior to September 11. In November 2001, Congress passed ATSA, which created TSA and gave it primary responsibility for securing all modes of transportation.[21]

[21] P.L. No. 107–71, 115 Stat. 597 (2001).

However, during TSA's first year of existence, TSA's main focus was on aviation security—more specifically, on meeting ATSA deadlines. While TSA was primarily focusing on aviation security, DOT modal administrations launched various initiatives to enhance the security of the maritime and land transportation modes. With the immediate crisis of meeting many aviation security deadlines behind it, TSA has been able to focus more on the security of all modes of transportation.

Legislation has not specifically defined TSA's role and responsibilities in securing all modes of transportation. In particular, ATSA does not specify TSA's role and responsibilities in securing the maritime and land transportation modes in detail as it does for aviation security. For instance, the act does not set deadlines for TSA to implement certain transit security requirements. Instead, the act simply states that TSA is responsible for ensuring security in all modes of transportation. The act also did not eliminate the existing statutory responsibilities for DOT modal administrations to secure the different transportation modes. Moreover, recent legislation indicates that DOT still has security responsibilities. In particular, the Homeland Security Act of 2002 states that the Secretary of Transportation is responsible for the security as well as the safety of rail and the transport of hazardous materials by all modes.

To clarify their roles and responsibilities in transportation security, DOT modal administrations and TSA planned to develop memorandums of agreement. The purpose of these documents was to define the roles and responsibilities of the different agencies for transportation security and address a variety of issues, including separating safety and security activities, interfacing with the transportation industry, and establishing funding priorities. TSA and the DOT modal administrations worked for months to develop the memorandums of agreement and the draft agreements were presented to senior DOT and TSA management for review in early spring of this year. According to DOT's General Counsel, with the exception of the memorandum of agreement between FAA and TSA, the draft memorandums were very general and did not provide much clarification. Consequently, DOT and TSA decided not to sign the memorandums of agreement, except for the memorandum of agreement between FAA and TSA, which was signed on February 28, 2003.[22]

The General Counsel suggested several reasons why the majority of the draft memorandums of agreement were too general. First, as TSA's departure date approached—that is, the date that TSA transferred from DOT to DHS—TSA and DOT modal administration officials may have grown concerned about formally binding the organizations to specific roles and responsibilities. Second, the working relationships between TSA and most of the DOT modal administrations are still very new; as a result, all of the potential issues, problem areas, or overlap have yet to be identified. Thus, identifying items to include in the memorandums of agreement was more difficult.

Rather than execute memorandums of agreement, the Secretary of Transportation and the Administrator of TSA exchanged correspondence that commits each entity to continued coordination and collaboration on security measures. In the correspondence, the Secretary and Administrator also agreed to use the memorandum of agreement between TSA and FAA as a framework for their interactions on security matters for all other modes. TSA and DOT officials stated that they believe memorandums of agreement are a good strategy for delineating roles and responsibilities and said that they would be open to using memorandums of agreement in the future.

Experts and Associations Identified Future Actions to Advance the Security of the Transportation System

Transportation security experts and representatives of state and local government and industry associations we contacted generally believe that the transportation system is more secure today than it was prior to September 11. Transportation stakeholders have worked hard to strengthen the security of the system. Nevertheless, transportation experts, industry representatives, and Federal officials all recommend that more work be done. Transportation experts and state and local government and industry representatives identified a number of actions that, in their view, the Federal Government should take to enhance security, including clarifying Federal roles and coordinating Federal efforts, developing a transportation security strategy, funding security enhancements, investing in research and development, and providing better intelligence information and related guidance. Specifically:

[22] DOT and TSA have signed other memorandums of agreement that are narrow in scope and address a specific issue. For example, TSA and DOT signed a memorandum of agreement regarding the processing of civil rights complaints.

- *Clarify Federal roles and responsibilities.* The lack of clarity about the roles and responsibilities of Federal entities in transportation security creates the potential for confusion, duplication, and conflicts. Understanding roles, responsibilities, and whom to call is crucial in an emergency. However, representatives from several industry associations stated that their members were unclear about which agency to contact for their various security concerns and which agency has oversight for certain issues. Furthermore, they said that they do not have contacts within these agencies. As mentioned earlier, several industry representatives reported that their members are receiving different messages from various Federal agencies involved in transportation security, which creates confusion and frustration within the industry. According to industry representatives and transportation security experts, uncertainty about Federal roles and the lack of coordination are straining intergovernmental relationships, draining resources, and raising the potential for problems in responding to terrorism. One industry association told us, for instance, that it has been asked by three different Federal agencies to participate in three separate studies of the same issue.
- *Establish a national transportation strategy.* A national strategy is crucial for helping stakeholders identify priorities, leveraging resources, establishing stakeholder performance expectations, and creating incentives for stakeholders to improve security. Currently, local government associations view the absence of performance expectations—coupled with limited threat information—as a major obstacle in focusing their people and resources on high-priority threats, particularly at elevated threat levels. The experts also noted that modal strategies—no matter how complete—cannot address the complete transportation security problem and will leave gaps in preparedness. As mentioned earlier, TSA is in the process of developing a national transportation system security plan,[23] which, according to the Deputy Administrator of TSA, will provide an overarching framework for the security of all modes.
- *Provide funding for needed security improvements.* Although an overall security strategy is a prerequisite to investing wisely, providing adequate funding also is essential, according to experts we contacted. Setting security goals and strategies without adequate funding diminishes stakeholders' commitment and willingness to absorb initial security investments and long-term operating costs, an expert emphasized. Industry and state and local government associations also commented that Federal funding should accompany any Federal security standards; otherwise, mandatory standards will be considered unfunded mandates that the industry and state and local governments will have to absorb.
- *Invest in research and development for transportation security.* According to most transportation security experts and associations we contacted, investing in research and development is an appropriate role for the Federal Government, because the products of research and development endeavors would likely benefit the entire transportation system, not just individual modes or operators. TSA is actively engaged in research and development projects, such as the development of the next generation explosive detection systems for baggage, hardening of aircraft and cargo/baggage containers, biometrics and other access control methods, and human factors initiatives to identify methods to improve screener performance, at its Transportation Security Laboratory in Atlantic City, New Jersey. However, TSA noted that continued adequate funding for research and development is paramount in order for TSA to be able to meet security demands with up-to-date and reliable technology.
- *Provide timely intelligence information and related guidance.* Representatives from numerous associations commented that the Federal Government needs to provide timely, localized, actionable intelligence information. They said that general threat warnings are not helpful. Rather, transportation operators want more specific intelligence information so that they can understand the true nature of a potential threat and implement appropriate security measures. Without more localized and actionable intelligence, stakeholders said they run the risk of wasting resources on unneeded security measures or not providing an adequate level of security. Moreover, local government officials often are not allowed to receive specific intelligence information because they do not have appropriate Federal security clearances. Also, there is little Federal guidance on how local authorities should respond to a specific threat or general threat warnings. For example, San Francisco police were stationed at the Golden Gate

[23] TSA hopes to have a draft of the national transportation system security plan prepared by the end of this year.

Bridge to respond to the elevated national threat condition. However, without information about the nature of the threat to San Francisco's large transportation infrastructure or clear Federal expectations for a response, it is difficult to judge whether actions like this are the most effective use of police protection, according to representatives from a local government association.

Observations

Securing the transportation system is fraught with challenges. Despite these challenges, transportation stakeholders have worked to strengthen security since September 11. However, more work is needed. It will take the collective effort of all transportation stakeholders to meet the continuing challenges and enhance the security of the transportation system.[24]

During TSA's first year of existence, it met a number of challenges, including successfully meeting many congressional deadlines for aviation security. With the immediate crisis of meeting these deadlines behind it, TSA can now examine the security of the entire transportation system. As TSA becomes more active in securing the maritime and land transportation modes, it will become even more important that the roles of TSA and DOT modal administrations are clearly defined. Lack of clearly defined roles among the Federal entities could lead to duplication and confusion. More importantly, it could hamper the transportation sector's ability to prepare for and respond to attacks. Therefore, in our report, we recommended that the Secretary of Homeland Security and the Secretary of Transportation develop mechanisms, such as a memorandum of agreement, to clearly define the roles and responsibilities of TSA and DOT in transportation security and communicate this information to stakeholders.

This concludes my prepared statement. I would be pleased to respond to any questions you or other Members of the Committee may have.

[24] See appendix III for a listing of active GAO engagements related to transportation security.

APPENDIX I

Key Actions Taken by DOT Modal Administrations to Secure the Different Transportation Modes, September 2001 to May 2003

Mode	DOT modal administration	Examples of actions taken
All (transport of hazardous materials)	Research and Special Programs Administration (Office of Hazardous Materials Safety)	• Established regulations for shippers and transporters of certain hazardous materials to develop and implement security plans and to require security awareness training for hazmat employees. • Developed hazardous materials transportation security awareness training for law enforcement, the industry, and the hazmat community. • Published security advisory, which identifies measures that could enhance the security of the transport of hazardous materials. • Investigated the security risks associated with placarding hazardous materials, including whether removing placards from certain shipments improve shipment security, and whether alternative methods for communicating safety hazards could be deployed.
Aviation	Federal Aviation Administration	• Established rule for strengthening cockpit doors on commercial aircraft. • Issued guidance to flight school operators for additional security measures. • Assisted Department of Justice in increasing background check requirements for foreign nationals seeking pilot certificates. • Increased access restrictions at air traffic control facilities. • Developed computer security strategy.
Highways	Federal Highway Administration	• Provided vulnerability assessment and emergency preparedness workshops. • Developed and prioritized list of highway security research and development projects. • Convened blue ribbon panel on bridge and tunnel vulnerabilities.
Maritime	U.S. Coast Guard[a]	• Activated and deployed port security units to help support local port security patrols in high threat areas. • Boarded and inspected ships to search for threats and confirmed the identity of those aboard. • Conducted initial assessments of the Nation's ports to identify vessel types and facilities that pose a high risk of being involved in a transportation security incident. • Established a new centralized National Vessel Movement Center to track the movement of all foreign-flagged vessels entering U.S. ports of call. • Established new guidelines for developing security plans and implementing security measures for passenger vessels and passenger terminals. • Used the pollution and hazardous materials expertise of the Coast Guard's National Strike Force to prepare for and respond to bioterrorism and weapons of mass destruction.
	Maritime Administration	• Increased port security and terrorism emphasis at National Port Readiness Network Port Readiness Exercises. • Provided port security training and developed standards and curriculum to educate and train maritime security personnel. • Increased access restrictions and established new security procedures for the Ready Reserve Force. • Provided merchant mariner background checks for Ready Reserve Force and sealift vessels in support of Department of Defense and Coast Guard requirements. • Provided merchant mariner force protection training.

Key Actions Taken by DOT Modal Administrations to Secure the Different Transportation Modes, September 2001 to May 2003—Continued

Mode	DOT modal administration	Examples of actions taken
Motor carrier	Federal Motor Carrier Safety Administration	• Conducted 31,000 on-site security sensitivity visits for hazardous materials carriers; made recommendations after visits. • Initiated a field operational test to evaluate different safety and security technologies and procedures, and identify the most cost-effective means for protecting different types of hazardous cargo for security purposes. • Provided free training on trucks and terrorism to law enforcement officials and industry representatives. • Conducted threat assessment of the hazardous materials industry.
Motor coach	Federal Motor Carrier Safety Administration	• Developed three courses for drivers on security-related information, including different threats, how to deal with packages, and how to respond in the case of an emergency.
Pipeline	Research and Special Programs Administration (Office of Pipeline Safety)	• Developed contact list of operators who own critical systems. • Convened blue ribbon panel with operators, state regulators, and unions to develop a better understanding of the pipeline system and coordinate efforts of the stakeholders. • Worked with TSA to develop inspection protocols to use for pipeline operator security inspections. The Office of Pipeline Safety and TSA have begun the inspection of major operators. • Created e:mail network of pipeline operators and a call-in telephone number that pipeline operators can use to obtain information. • Directed pipeline operators to identify critical facilities and develop security plans for critical facilities that address deterrence, preparedness, and rapid response and recovery from attacks. • Worked with industry to develop risk-based security guidance, which is tied to national threat levels and includes voluntary, recommended countermeasures.
Rail	Federal Railroad Administration	• Reviewed Association of American Railroads' and Amtrak's security plans. • Assisted commuter railroads with their security plans. • Provided funding for security assessments of three commuter railroads, which were included in FTA's assessment efforts. • Reached out to international community for lessons learned in rail security.
Transit	Federal Transit Administration	• Shared threat information with railroads and rail labor. • Awarded $3.4 million in grants to over 80 transit agencies for emergency response drills. • Offered free security training to transit agencies. • Conducted security assessments at the 36 largest transit agencies. • Provided technical assistance to 19, with a goal of 60, transit agencies on security and emergency plans and emergency response drills. • Increased funding for security research and development efforts.

Source: GAO presentation of information provided by DOT modal administrations.
[a]The U.S. Coast Guard was transferred to DHS in the Homeland Security Act of 2002 (P.L. No. 107–296, 116 Stat. 2135 (2002)).

APPENDIX II

Elements of a Risk Management Approach

A risk management approach encompasses three key elements—a threat assessment, vulnerability assessment, and criticality assessment. In particular, these three elements provide the following information:

- A threat assessment identifies and evaluates potential threats on the basis of such factors as capabilities, intentions, and past activities. This assessment represents a systematic approach to identifying potential threats before they materialize. However, even if updated often, a threat assessment might not adequately capture some emerging threats. The risk management approach, therefore, uses vulnerability and critical assessments as additional input to the decision-making process.
- A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses.
- A criticality assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy. The assessment provides a basis for identifying which structures or processes are relatively more important to protect from attack. Thus, it helps managers determine operational requirements and target resources to the highest priorities while reducing the potential for targeting resources to lower priorities.

APPENDIX III

GAO Active Engagements Related to Transportation Security

TSA Baggage Screening

Key Questions: (1) What are the status and associated costs of TSA efforts to acquire, install, and operate explosive detection equipment (Electronic Trace Detection Technology and Explosive Detection Systems) to screen all checked baggage by December 31, 2003? (2) What are the benefit and tradeoffs—to include costs, operations and performance—of using alternative explosive detection technologies currently available for baggage screening?

General Aviation Security

Key Questions: (1) How has security concerns and measures at changed at general aviation airports since September 11, 2001? (2) What steps has the Transportation Security Administration taken to improve general aviation security?

Banner Pilot Waivers

Key Questions: (1) What are procedures for conducting background and security checks for pilots of small banner-towing aircraft requesting waivers to perform stadium overflights? (2) To what extent were these procedures followed in conducting required background and security checks since 9/11? (3) How effective were these procedures in reducing risks to public safety?

U.S. Coast Guard Budget And Mission Performance

Key Questions: (1) What are the levels of effort for USCG's various missions? (2) What is USCG's progress in developing a strategic plan for setting goals for all of its various missions? (3) What is USCG's mission performance as compared to its performance and strategic plans?

Transportation Security Administration's Computer Assisted Passenger Prescreening System II (CAPPS–II)

Key Questions: (1) How will the CAPPS–II system function and what data will be needed to make the system operationally effective? (2) What safeguards will be put in place to protect the traveling public's privacy? (3) What systems and measures are in place to determine whether CAPPS–II will result in improved national security? (4) What impact will CAPPS–II have on the traveling public and airline industry in terms of costs, delays, risks, and hassle, etc.?

Transportation Security Administration Passengers Screening Program

Key Questions: (1) What efforts have been taken or planned to ensure passenger screeners comply with Federal standards and other criteria, to include efforts to train, equip, and supervise passenger screeners? (2) What methods does TSA use to test screener performance, and what have been the results of these tests? (3) How have the results of tests of TSA passenger screeners compared to the results achieved by screeners prior to 9/11 and at the 5 pilot program airports? (4) What actions are TSA taking to remedy performance concerns?

TSA's Use of Sole Source Contracts

Key Questions: (1) To what extent does TSA follow applicable acquisition laws and policies, including ensuring adequate competition? (2) How well does TSA's organizational structure facilitate effective, efficient procurement? (3) How does TSA ensure that its acquisition workforce is equipped to award and oversee contracts? (4) How well do TSA's policies and processes ensure that it receives the supplies and services it needs on time and at reasonable cost?

TSA's Efforts to Implement Section 106, 136, and 138 of the Aviation and Transportation Security Act

Key Questions: (1) What is the status of TSA's efforts to implement section 106 of the Act requiring improved airport perimeter access security? (2) What is the status of TSA's efforts to implement section 136 requiring assessment and deployment of commercially available security practices and technologies? (3) What is the status of TSA's efforts to implement section 138 requiring background investigations for TSA and other airport employees?

Implementation of the Maritime Transportation Security Act of 2002

Key Questions: (1) How effectively is the port vulnerability assessment process being implemented, and what actions are being taken to address deficiencies identified? (2) What progress is being made to develop port, vessel, and facility security plans? (3) Does the CG have sufficient resources and an action plan to ensure the plans be completed, reviewed and approved in time to meet statutory deadlines? (4) What will it cost stakeholders to comply?

Assessment of the Portable Air Defense Missile Threat

Key Questions: (1) What is the nature and extent of the threat from MANPADs? (2) How effective are U.S. controls on the use of exported MANPADs? (3) How do multilateral efforts attempt to stem MANPAD proliferation? (4) What types of countermeasures are available to minimize this threat and at what cost?

Federal Aviation Administration Designee Program

Key Questions: (1) What is the nature, scope, and operational framework of the designee program? (2) What are the identified strengths and weaknesses of the program? (3) What is the potential for FAA's ODA proposal and other stakeholders' alternatives to address the identified program weaknesses?

Custom Cargo Inspections at Seaports

Key Questions: (1) How has Customs developed the Automated Targeting System (ATS) and the new anti-terrorism rules? (2) How does Customs use ATS to identify containerized cargo as "high risk" for screening and inspection to detect cargo that might contain weapons of mass destruction (WMD)? (3) To what extent is ATS implemented at seaports, including impact and challenges involved? (4) What is Customs' plan for assessing system implementation and performance?

Enhancement Options for Intermodal Freight Transportation

Key Questions: (1) What are the current and emerging national challenges to freight mobility and what proposals have been put forth to address these issues? (2) To what extent do these current and emerging challenges exist at container ports and surrounding areas and to what extent do the proposals appear to have applicability to these locations?

Social Security Administration's Role in Verifying Identities for State's Licensing of Drivers

Key Questions: (1) What are states' policies and practices for verifying the identity of driver's license/ID card applicants and how might they more effectively use SSNs or other tools to verify identity? (2) How does SSA assist states in verifying SSNs for driver's license/ID card applicants and how can SSA improve the verification service it provides?

United States Coast Guard's National Distress and Response "Rescue 21" System Modernization

Key Questions: (1) What are the status, plans, and technical and programmatic risks associated with the National Distress and Response System (NDRS) Modernization Project? (2) How is the Coast Guard addressing concerns with the new NDRS, such as communication coverage gaps and the inability to pinpoint distressed boaters? (3) How will Coast Guard's new homeland security role affect the NDRS project?

U.S. Border Radiation Detection

Key Questions: (1) What is the status of Customs' plan to install radiation detection equipment at U.S. border crossings? (2) What is the basis for the plan's time frame? (3) What is Customs' technical capability to implement the plan? (4) How well is Customs coordinating with other agencies in the area of radiation detection? (5) What are the results of Customs' evaluations of radiation detection equipment and how are the evaluations being used?

Airline Assistance Determination of Whether the $5 Billion Provided by P.L. 107–42 Was Used to Compensate the Nation's Major Air Carriers for Their Losses Stemming from the Events of Sept. 11, 2001

Key Questions: (1) Was the $5 billion used only to compensate major air carriers for their uninsured losses incurred as a result of the terrorist attacks? (2) Were carriers reimbursed, per the act, only for increases in insurance premiums resulting from the attacks?

Effectiveness of the Transportation Security Administration's Research and Development Program

Key Questions: (1) What is the budget profile for the Federal Aviation Administration's and the Transportation Security Administration's (TSA's) aviation security research and development (R&D) program? (2) How effective is TSA's strategy for determining which aviation security technologies to research and develop? (3) To what extent do stakeholders believe that TSA is researching and developing the most promising aviation security technologies?

Federal Air Marshals

Key Questions: (1) How has the FAM program evolved, in terms of recruiting, training, retention, and operations since the transfer of program management to TSA? (2) To what extent has TSA implemented the necessary internal controls to meet the human capital and operational challenges of the FAM program? (3) To what extent has TSA developed plans and initiatives to accommodate future FAM program sustainability, growth and maturation?

RELATED GAO PRODUCTS

Transportation Security Reports and Testimonies

Transportation Security: Federal Action Needed to Help Address Security Challenges, GAO–03–843 (Washington, D.C.: June 30, 2003).

Transportation Security Research: Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments, GAO–03–502 (Washington, D.C.: May 1, 2003).

Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed, GAO–03–435 (Washington, D.C.: April 30, 2003).

Coast Guard: Challenges during the Transition to the Department of Homeland Security, GAO–03–594T (Washington, D.C.: April 1, 2003).

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges, GAO–03–616T (Washington, D.C.: April 1, 2003).

Aviation Security: Measures Needed to Improve Security of Pilot Certification Process, GAO–03–248NI (Washington, D.C.: February 3, 2003). (Not for Public Dissemination)

Major Management Challenges and Program Risks: Department of Transportation, GAO–03–108 (Washington, D.C.: January 1, 2003).

High Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructure, GAO–03–121 (Washington, D.C.: January 1, 2003).

Aviation Safety: Undeclared Air Shipments of Dangerous Goods and DOT's Enforcement Approach, GAO–03–22 (Washington, D.C.: January 10, 2003).

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System, GAO–03–344 (Washington, D.C.: December 20, 2002).

Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges, GAO–03–263 (Washington, D.C.: December 13, 2002).

Aviation Security: Registered Traveler Program Policy and Implementation Issues, GAO–03–253 (Washington, D.C.: November 22, 2002).

Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk, GAO–03–303T (Washington, D.C.: November 19, 2002).

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges, GAO–03–297T (Washington, D.C.: November 18, 2002).

Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions, GAO–03–155 (Washington, D.C.: November 12, 2002).

Mass Transit: Challenges in Securing Transit Systems, GAO–02–1075T (Washington, D.C.: September 18, 2002).

Pipeline Safety and Security: Improved Workforce Planning and Communication Needed, GAO–02–785 (Washington, D.C.: August 26, 2002).

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful, GAO–02–993T (Washington, D.C.: August 5, 2002).

Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges, GAO–02–971T (Washington, D.C.: July 25, 2002).

Critical infrastructure Protection: Significant Challenges Need to Be Addressed, GAO–02–961T (Washington, D.C.: July 24, 2002).

Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports, GAO–02–955TNI (Washington, D.C.: July 23, 2002). (Not for Public Dissemination)

Information Concerning the Arming of Commercial Pilots, GA0–02–822R (Washington, D.C.: June 28, 2002).

Aviation Security: Deployment and Capabilities of Explosive Detection Equipment, GAO–02–713C (Washington, D.C.: June 20, 2002). (Classified)

Coast Guard: Budget and Management Challenges for 2003 and Beyond, GAO–02–538T (Washington, D.C.: March 19, 2002).

Aviation Security: Information on Vulnerabilities in the Nation's Air Transportation System, GAO–01–1164T (Washington, D.C.: September 26, 2001). (Not for Public Dissemination)

Aviation Security: Information on the Nation's Air Transportation System Vulnerabilities, GAO–01–1174T (Washington, D.C.: September 26, 2001). (Not for Public Dissemination)

Aviation Security: Vulnerabilities in, and Alternatives for, Preboard Screening Security Operations, GAO–01–1171T (Washington, D.C.: September 25, 2001).

Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities, GAO–01–1165T (Washington, D.C.: September 21, 2001).

Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security, GAO–01–1166T (Washington, D.C.: September 20, 2001).

Aviation Security: Terrorist Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports, GAO–01–1162T (Washington, D.C.: September 20, 2001).

Terrorism and Risk Management

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues, GAO–03–715T (Washington, D.C.: May 8, 2003).

Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture, GAO–03–190 (Washington, D.C.: January 17, 2003).

Homeland Security: Management Challenges Facing Federal Leadership, GAO–03–260 (Washington, D.C.: December 20, 2002).

Homeland Security: Information Technology Funding and Associated Management Issues, GAO–03–250 (Washington, D.C.: December 13, 2002).

Homeland Security: Information Sharing Activities Face Continued Management Challenges, GAO–02–1122T (Washington, D.C.: October 1, 2002).

National Preparedness: Technology and Information Sharing Challenges, GAO–02–1048R (Washington, D.C.: August 30, 2002).

Homeland Security: Effective Intergovernmental Coordination Is Key to Success, GAO–02–1013T (Washington, D.C.: August 23, 2002).

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems, GAO–02–474 (Washington, D.C.: July 15, 2002).

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed, GAO–02–918T (Washington, D.C.: July 9, 2002).

Homeland Security: Intergovernmental Coordination and Partnership Will Be Critical to Success, GAO–02–901T (Washington, D.C.: July 3, 2002).

Homeland Security: New Department Could Improve Coordination but May Complicate Priority Setting, GAO–02–893T (Washington, D.C.: June 28, 2002).

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy, GAO–02–811T (Washington, D.C.: June 7, 2002).

Homeland Security: Responsibility and Accountability for Achieving National Goals, GAO–02–627T (Washington, D.C.: April 11, 2002).

National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts is Critical to an Effective National Strategy for Homeland Security, GAO–02–621T (Washington, D.C.: April 11, 2002).

Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness, GAO–02–550T (Washington, D.C.: April 2, 2002).

Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy, GAO–02–549T (Washington, D.C.: March 28, 2002).

Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness, GAO–02–548T (Washington, D.C.: March 25, 2002).

Combating Terrorism: Intergovernmental Partnership in a National Strategy to Enhance State and Local Preparedness, GAO–02–547T (Washington, D.C.: March 22, 2002).

Homeland Security: Progress Made; More Direction and Partnership Sought, GAO–02–490T (Washington, D.C.: March 12, 2002).

Combating Terrorism: Key Aspects of a National Strategy to Enhance State and Local Preparedness, GAO–02–473T (Washington, D.C.: March 1, 2002).

Homeland Security: Challenges and Strategies in Addressing Short-and Long-Term National Needs, GAO–02–160T (Washington, D.C.: November 7, 2001).

Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts, GAO–02–208T (Washington, D.C.: October 31, 2001).

Combating Terrorism: Considerations for Investing Resources in Chemical and Biological Preparedness, GAO–02–162T (Washington, D.C.: October 17, 2001).

Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, GAO–02–24 (Washington, D.C.: October 15, 2001).

Homeland Security: Key Elements of a Risk Management Approach, GAO–02–150T (Washington, D.C.: October 12, 2001).

Chemical and Biological Defense: Improved Risk Assessment and Inventory Management Are Needed, GAO–01–667 (Washington, D.C.: September 28, 2001).

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks, GAO–01–1168T (Washington, D.C.: September 26, 2001).

Homeland Security: A Framework for Addressing the Nation's Efforts, GAO–01–1158T (Washington, D.C.: September 21, 2001).

Combating Terrorism: Selected Challenges and Related Recommendations, GAO–01–822 (Washington, D.C.: September 20, 2001).

Senator LOTT [presiding]. Mr. Dillingham and Ms. Wrightson, I believe you're just with Mr. Guerrero for possible questions later on. Thank you very much for being here.

[The prepared statements of Ms. Wrightson and Mr. Dillingham follow:]

PREPARED STATEMENT OF MARGARET WRIGHTSON, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, UNITED STATES GENERAL ACCOUNTING OFFICE

PROGRESS MADE IN IMPLEMENTING MARITIME TRANSPORTATION SECURITY ACT, BUT CONCERNS REMAIN

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss the implementation of the Maritime Transportation Security Act (MTSA) of 2002. This sweeping piece of legislation was enacted just 10 months ago, but it has already produced major changes in the Nation's approach to maritime security. At your request, we have begun reviewing the implementation of security provisions of Title I of MTSA. I am here today to tell you about our preliminary findings and what agencies within the Department of Homeland Security (DHS) and other Federal departments are doing to fulfill their many responsibilities under the act. I also want to advise you about specific matters that agency officials or others have brought to our attention thus far and other issues that may require further oversight. We will be continuing our efforts to more fully evaluate a number of the issues I will address today, and we plan to issue a report when this work is complete.

Our information is based on interviews with agency officials charged with implementing MTSA's provisions, as well as with officials and stakeholders from several ports.

Our preliminary findings are as follows:

- Progress has been made in implementing MTSA. MTSA called for actions in 46 key areas we identified, such as creating a maritime intelligence security system, assessing security conditions in port areas, creating and implementing a vessel tracking system, and creating identification systems for port workers and seafarers. So far, we have obtained information for 43 of these areas, and agency officials indicate that actions are complete or under way in 42 of them. For example, the Coast Guard, which had lead responsibility for most of the assignments, has six interim rules in place covering major areas of responsibility, such as security in and around the ports, aboard individual vessels, and at individual facilities. All six Coast Guard Maritime Safety and Security Teams included in the Fiscal Year 2003 budget are expected to be operational by the end of September 2003; these teams are designed to provide increased protection against terrorism in and around the Nation's harbors. Also, the Transportation Security Administration (TSA) is testing new identification cards for controlling access to secure transportation facilities, including vessels and port facilities. The agency plans to start issuing the cards to millions of port workers in 2004. The Bureau of Customs and Border Protection (BCBP) and the Maritime Administration (MARAD), the two other agencies with the largest set of responsibilities under MTSA, also are making progress on major projects. Agency officials told us that cooperation and coordination on MTSA implementation has been strong. Further work will be needed to determine the extent to which early progress will be sustained over the course of implementation efforts and whether the spirit of cooperation translates into efforts at the port level.
- These findings not withstanding and bearing in mind our caveats as to the preliminary nature of these results, five areas have surfaced as potentially requiring further attention. (See table 1.)

Table 1.—Summary of Areas That Require Further Attention

Area	Description
Security-related matters	
Vessel identification system	A system has been developed and is being implemented, but the shore-based infrastructure needed is not present at many U.S. ports. As a result, the system may not be in place at these ports for several years.
Port security assessments	Assessments being conducted by an outside contractor have been criticized for their scope and quality, and the contractor has attempted to move to the next phase of the work before evaluating essons learned.
Vessel security plans	Concerns have been raised about the Coast Guard's plan to accept other countries' certification of vessel security plans.
Operational and efficiency matters	
Maritime intelligence system	Coast Guard and Transportation Security Administration may be duplicating efforts in collecting intelligence information about vessels and cargoes.
Grants program	A MTSA-required program of grants for assisting in security preparations is being folded into an existing grants program, affecting the application of MTSA grant requirements.

Source: GAO.

Three of these areas, as shown in table 1, primarily have security implications. For example, MTSA called for development of an automatic identification system. The Coast Guard developed a system that would allow port officials and personnel on other vessels to determine the identity and position of vessels entering or operating within the port. While the Coast Guard is implementing this system, more than half of the 25 busiest U.S. ports will not have it for the foreseeable future, because it requires extensive shore-based equipment and infrastructure that many ports do not have. The two remaining areas relate primarily to operational or efficiency matters, such as duplication of effort in collecting intelligence information. We are continuing to examine all five areas.

Background

MTSA was landmark legislation that mandated a quantum leap in security preparedness for America's maritime ports. Prior to the terrorist attacks of September 11, 2001, Federal attention at ports tended to focus on navigation and safety issues, such as dredging channels and environmental protection. While the terrorist attacks initially focused the Nation's attention on the vulnerability of its aviation system, it did not take long for attention to fall on the Nation's ports as well. Besides being gateways through which dangerous materials could enter the country, ports represent attractive targets for other reasons: they are often large and sprawling, accessible by water and land, close to crowded metropolitan centers, and interwoven with highways, roads, factories, and businesses. Security is made more difficult by the many stakeholders, public and private, involved in port operations. These stakeholders include local, state, and Federal agencies; multiple law enforcement jurisdictions; transportation and trade companies; and factories and other businesses.

Passed in November 2002, MTSA imposed an ambitious schedule of requirements on a number of Federal agencies. MTSA called for a comprehensive security framework—one that included planning, personnel security, and careful monitoring of vessels and cargo. (See table 2 for examples of key MTSA activities.) MTSA tasked the Secretary of DHS, and the Secretary in turn has tasked the Coast Guard, with lead responsibility for the majority of its requirements. Timetables were often daunting. For example, one of the Coast Guard's responsibilities was to develop six interim final rules implementing MTSA's operational provisions in sufficient time to receive public comment and to issue a final rule by November 25, 2003.

Table 2.—Examples of Key MTSA Activities

Type of activity	Specific provision
Planning	
	Conduct vessel, facility, and port vulnerability assessments to determine potential risks.
	Develop transportation security plans for vessels, facilities, port areas, and the Nation.
	Develop security incident response plans for vessels and facilities.
	Assess foreign ports for security risk.
Identification of personnel	
	Create security cards required of any person seeking to enter a secure area of a vessel or facility; cards would have biometric information (such as fingerprint data) to guard against theft or counterfeiting.
Tracking of vessels	
	Install automatic identification systems on numerous categories of vessels.
	Authorized to create and implement a long-range vessel tracking system.

Source: GAO.

Adding to the difficulty has been the need to implement MTSA against the backdrop of the most extensive Federal reorganization in over a half-century. Most of the agencies with MTSA responsibilities were reorganized into the Department of Homeland Security in March 2003, less than 5 months after MTSA enactment. Among the 22 agencies in the new department were some relatively new organizations, such as TSA. Other more longstanding agencies, including the Coast Guard, U.S. Customs Service, and Immigration and Naturalization Service, were transferred from a variety of executive departments. This vast recombination of organizational cultures introduced new chains of command and reporting responsibilities. MTSA implementation also involved coordination with other executive agencies, including the Departments of State, Transportation, and Justice.

Progress Has Been Made in Implementing MTSA

Since the passage of MTSA in 2002 the responsible agencies—primarily the Coast Guard, TSA, and BCBP in DHS, along with MARAD in the Department of Transportation—have made strides in implementing the act's security provisions. MTSA called for actions in 46 key areas we identified. Thus far, we have received information from the responsible agencies on 43 of these areas. Of the 43 areas, work is done in 2 (issuing interim rules and developing training for maritime security personnel), and under way in 40 others.[1] These agencies also reported that cooperation and coordination has been extensive throughout the course of their activities.

A major achievement has been the Coast Guard's publication on July 1, 2003, of six interim rules on the provisions where it had lead responsibility. The rules set requirements for many of the provisions delegated to the Coast Guard under MTSA. The rules, which included sections on national maritime security initiatives, area maritime security, vessel security, facility security, outer continental shelf facility security, and automatic identification systems, were published approximately 8 months after MTSA was enacted. Doing so kept the Coast Guard on schedule for meeting MTSA's requirement to receive public comment and issue the final rules by the end of November 2003. The rules provided a comprehensive description of industry-related maritime security requirements and the cost-benefit assessments of the entire set of rules. The Coast Guard plans to publish the final rules before November 25, 2003, after receiving and acting on comments to the interim rules.

Another Coast Guard accomplishment was the establishment of Maritime Safety and Security Teams called for under MTSA. These teams, which can be rapidly deployed where needed, are designed to provide antiterrorism protection for strategic shipping, high-interest vessels, and critical infrastructure. The Coast Guard has already deployed four teams—in Seattle and Galveston and near Norfolk and Los An-

[1] Work has not yet begun on issuing a report to the Congress regarding MARAD's expenditure of funds for training—no funds were expended in Fiscal Year 2003.

geles. The Coast Guard will deploy teams in New York City and near Jacksonville this year, and six more teams have been requested in the president's budget in 2004. These are to be located in San Diego, Honolulu, Boston, San Francisco, New Orleans, and Miami.

Other agencies in DHS have also made progress in their implementation of MTSA provisions. Responding to MTSA's requirement for the development of biometric[2] transportation security identification cards that would allow only authorized persons access to secure areas of vessels or facilities, TSA is currently testing several different technology credentialing systems on sample cards. The agency will begin testing prototypes of the entire security card process, including conducting background checks, collecting biometric information on workers, verifying cardholders' identities, and issuing cards in early 2004. TSA plans to start issuing about 5 to 6 million new cards per year in the middle of 2004. Developing all of the policies and programs to make this system work is still under way and will continue to pose challenges to continued progress. Another DHS agency, BCBP, was delegated the responsibility for issuing regulations for electronic transmission of cargo information to BCBP by October 1, 2003; BCBP published its proposed rule on July 23, 2003. BCBP was waiting for comments on the proposed rule, and BCBP officials told us that they expect to publish the rule on time.

MARAD has also made progress in its requirements. Among the provisions for which MARAD is responsible are developing standards and curricula for the training of maritime security personnel. MARAD submitted a Report to Congress, dated May 2003, containing the standards and curriculum called for by MTSA in the form of model course frameworks for seven categories of maritime security professionals. As an extension of the MTSA project, MARAD also produced three model maritime security courses for the International Maritime Organization (IMO). An IMO validation team has reviewed drafts of these courses, which found little need for change.

Agency officials told us that cooperation and coordination on MTSA implementation has been strong. Coast Guard officials said that they had developed channels of communication with other relevant agencies, and they said these other agencies were supportive in implementing provisions for which they did not have primary responsibility. In the work we have conducted at ports since the September 11 attacks, we have noted an increasing level of cooperation and coordination at the port level. However, ensuring smooth coordination as the many aspects of MTSA implementation continue is a considerable challenge. Additional work will be needed to determine the extent to which this spirit of cooperation continues to be translated into effective actions at the level where programs must be implemented.

Issues Raised Include Both Security and Operational Concerns

While progress is being made, our preliminary work has identified five areas that merit attention and further oversight. Three relate primarily to security issues: (1) the limited number of ports that will be covered by the vessel identification system, (2) questions about the scope and quality of port security assessments, and (3) the Coast Guard's plans not to individually approve security plans for foreign vessels. The remaining two relate primarily to operational and efficiency matters: (1) potential duplication of maritime intelligence efforts and (2) inconsistency with Port Security Grant Program requirements.

Vessel Identification System Will Cover a Limited Number of Ports

The main security-related issue involves the implementation of a vessel identification system. MTSA called for the development of an automatic identification system. Coast Guard implementation calls for a system that would allow port officials and other vessels to determine the identity and position of vessels entering or operating within the harbor area. Such a system would provide an "early warning" of an unidentified vessel or a vessel that was in a location where it should not be. To implement the system effectively, however, requires considerable land-based equipment and other infrastructure that is not currently available in many ports. As a result, for the foreseeable future, the system will be available in less than half of the 25 busiest U.S. ports.

The identification system, called the Automatic Identification System (AIS), uses a device aboard a vessel to transmit a unique identifying signal to a receiver located at the port and to other ships in the area. This information gives port officials and other vessels nearly instantaneous information about a vessel's identity, position,

[2] Biometric refers to technologies that can be used to verify a person's identity by characteristics such as fingerprints, eye retinas, and voice.

speed, and course. MTSA requires that vessels in certain categories[3] install tracking equipment between January 1, 2003, and December 31, 2004, with the specific date dependent on the type of vessel and when it was built.

The only ports with the necessary infrastructure to use AIS are those that have waterways controlled by Vessel Traffic Service (VTS) systems. Similar to air traffic control systems, VTS uses radar, closed circuit television, radiophones, and other technology to allow monitoring and management of vessel traffic from a central shore-based location. The Coast Guard currently plans to install AIS receiving equipment at the 10 locations with VTS systems.[4] More than half of the 25 busiest ports, such as Philadelphia, Baltimore, Miami, Charleston, Tampa, and Honolulu, do not have VTS systems; hence, AIS will be inoperable at these locations for the foreseeable future. When AIS will be operable at these other ports depends heavily on how soon the Coast Guard can put an extensive amount of shore-based infrastructure in place. For the present, the Coast Guard is requiring AIS equipment only for (1) vessels on international voyages and (2) vessels navigating waterways under VTS control. Some of these international ships will be calling on ports that will not have AIS equipment. In such cases, the transmitters aboard the vessels will be of no use for the ports, because they will not have equipment to receive the signals.[5]

Cost is a major factor in the full implementation of AIS. Expanding coverage will require substantial additional investment, both public and private. The Coast Guard's budget request for Fiscal Year 2004 includes $40 million for shore-based AIS equipment and related infrastructure—an amount that covers only current VTS areas. According to a Coast Guard official, wider-reaching national implementation of AIS would involve installation and training costs ranging from $62 million to $120 million. Also, the cost of installing AIS equipment aboard individual ships averages about $10,000 per vessel, which is to be borne by the vessel owner or operator. Some owners and operators, particularly of domestic vessels, have complained about the cost of equipping their vessels.

Concerns about Port Security Assessments

Another security-related issue involves the Coast Guard's efforts to address MTSA's security planning requirements through a series of security assessments of individual ports. Security assessments are intended to be in-depth examinations of security threats, vulnerabilities, consequences, and conditions throughout a port, including not just transportation facilities, but also factories and other installations that pose potential security risks. The Coast Guard had begun these assessments before MTSA was passed and decided to continue the process, changing it as needed to meet MTSA planning requirements, which include developing area security plans based on the evaluation of specific facilities throughout the port. At the request of the Subcommittee on Coast Guard and Maritime Transportation, House Committee on Transportation and Infrastructure, we have been examining these assessments, which are being conducted by an outside contractor. Our preliminary work has surfaced several potential concerns, which we are still in the process of reviewing.

One concern involves an apparent truncation of the review process for ensuring that the assessment methodology will deliver what MTSA requires. When MTSA took effect, the outside contractor already completed the first 10 of 55 planned assessments. The Coast Guard directed the contractor to modify the assessment methodology to take MTSA's planning requirements into account, and it decided that the next two assessments would be a pilot test of the revised methodology. The Coast Guard plans to use the pilot test to evaluate lessons learned, so that additional modifications can be made before any further contracts are signed.

Instead of waiting to see what changes might be needed as a result of the pilot projects, however, the contractor has apparently started the scoping phase for the next six port assessments. Scoping is a significant part of the new methodology, and as such, it is a major determinant in the nature and breadth of the issues to be addressed, as well as the assessment's cost. The contractor has also reportedly

---

[3] All vessels of certain specifications on international voyages; self-propelled commercial vessels 65 feet or more in length; towing vessels 26 feet or more in length and more than 600 horsepower; vessels of 100 gross tons or more carrying one or more passengers for hire; and passenger vessels certificated to carry 50 or more passengers for hire.

[4] These locations are New York/New Jersey; the mouth of the Mississippi River; New Orleans; Houston/Galveston; Port Arthur, Texas; Los Angeles/Long Beach; San Francisco; Seattle/Tacoma; Alaska's Prince William Sound; and Sault Ste. Marie, Michigan.

[5] Under Coast Guard rules, all vessels arriving from foreign ports must inform a U.S. port, at least 96 hours in advance, of its intent to enter the harbor. Ports without AIS will still have this notice; what they will lack is the ability to verify ships' identities electronically when they arrive, or to quickly identify ships that are attempting to arrive unidentified.

sought to negotiate and sign contracts to review the next six ports. Since the pilot projects will not be completed until at least October 2003, it seems premature to reach decisions about the scope of the assessments and sign contracts for them. The revised methodology needs to be reviewed so that any needed changes are reflected in the next contract.

A second concern that has surfaced involves the scope and quality of the assessments themselves. As part of our work, we have interviewed port stakeholders to obtain their views on the process. At one port, where the assessment has been completed and the report issued, stakeholders said they had not been given an opportunity to comment on the report, which contained factual errors and did not include an assessment of railroads and the local power generating plant. At the other port, where the assessment was still in process, local Coast Guard personnel and port stakeholders noted that a survey instrument referred to the wrong port, asked questions they regarded as not pertaining to security, and was conducted in ways that raised concerns about credibility. Many of these stakeholders saw little usefulness in the assessments, believing that they added little to what the stakeholders had already learned from conducting their own more extensive security reviews of individual facilities or installations. They said the assessments focused on the same systems that had already been reviewed and would have greater value if they were focused on matters that had not already been thoroughly studied, such as the potential for waterborne assault. Coast Guard officials at the two ports said, however, that in their view the assessments would provide such benefits as a more comprehensive perspective on port operations and vulnerabilities and validate their need for additional assets and people to provide adequate security. Ensuring that the assessments are of high quality is important not only for their effectiveness as security instruments, but also because of their cost. For the most part, assessments have been conducted only at medium-sized ports, and even there they are costing $1 million or more per assessment.

Coast Guard Not Intending to Individually Approve Security Plans for Foreign Vessels

Concerns have been raised about the proposed approach for meeting MTSA's requirement that the Secretary of DHS approve vessel security plans for all vessels operating in U.S. waters. Vessel security plans include taking such steps as responding to assessed vulnerabilities, designating security officers, conducting training and drills, and ensuring that appropriate preventive measures will be taken against security incidents. To implement this MTSA requirement the Coast Guard has stated, in general, that it is not the Coast Guard's intent to individually approve vessel security plans for foreign vessels. Separate from MTSA, an international agreement requires vessels to carry on board a vessel security plan that is approved by the vessel's country of registry—its "flag" state—to ensure that an acceptable security plan is in place. The Coast Guard provides that it will deem a flag state approval of a vessel security plan to constitute the MTSA-required Secretary approval of MTSA vessel security plans. However, MTSA does not mention any role for foreign nations in the Secretary's required approval of vessel security plans, and some concerns have been raised about the advisability of allowing flag states—some with a history of lax regulation—to ensure the security of vessels traveling to the United States.

The international requirement for a security plan is contained in the International Ship and Port Facility Security (ISPS) Code.[6] Under this requirement, which was adopted about the same time that MTSA was enacted and will go into effect on July 1, 2004, the vessel's flag state is responsible for reviewing and certifying the vessel's security plan. Prior to this time, the vessels' flag state had already been responsible for ensuring that its vessels met safety requirements. Critics of using this approach for MTSA-required security plans have pointed out that in the past, some flag states had a spotty record of enforcing safety requirements.

Rather than individually approving security plans for vessels overseen by foreign flag states, the Coast Guard plans an extensive monitoring effort as part of its oversight of vessels bound for U.S. waters. However, the Coast Guard's interim rule stated that, as part of an aggressive port state control program, the Coast Guard would verify that foreign vessels have an approved, fully implemented security plan, as well as tracking the performance of owners, operators, flag administrations, charters, and port facilities. Coast Guard officials have said that they are working from existing procedures, in that their security effort is modeled after their safety pro-

[6] This code was ratified by the International Maritime Organization, to which the United States is a party.

gram. They also said, however, that they have no contingency plans in case stronger measures than those called for in their current plans are required.

The concerns are limited mainly to foreign flag vessels. Vessels registered in the United States will have their security plans reviewed and approved by the Coast Guard. It has been reported that the Coast Guard estimates that review and approval of security plans for domestic vessels and facilities will require 150 full-time personnel and cost $70 million as part of its 2004 budget.

Potential Duplication of Maritime Intelligence Efforts

Turning to issues that are related more to program efficiency and management than to security concerns, one issue that has arisen involves potential duplication in the area of maritime intelligence. MTSA required the Secretary of Homeland Security to implement a system to collect, integrate, and analyze information on vessels operating on or bound for U.S. waters. The Secretary of DHS in turn delegated responsibilities to TSA and the Coast Guard. There appears to be potential for duplication by TSA and the Coast Guard in these efforts.

The duplication concerns center on the new Integrated Maritime Information System (IMIS) required under the Secretary's delegations. The Secretary of DHS delegated primary responsibility for this system to TSA, and TSA was appropriated $25 million to develop it. Coast Guard officials have voiced concerns that TSA's efforts in developing the overall system are duplicating existing Coast Guard efforts that are more extensive and better funded. According to these officials, IMIS is very similar to the Coast Guard's Intelligence Coordination Center (ICC) Coastwatch program, an effort that has 10 times the amount of funding appropriated for IMIS, involves 100 more staff members, and has staff already in place with considerable intelligence analysis capability. Coast Guard officials questioned whether TSA's smaller effort could yield information of similar quality.

Coast Guard officials also expressed concerns about potential duplication of effort at the port level. TSA's tests of the system would place TSA personnel at the port level. Coast Guard personnel noted that these efforts seemed similar to the Coast Guard's Field Intelligence Support Teams, as well as teams from the legacy agencies, the Customs Service and the Immigration and Naturalization Service, that also operate at the port level. Coast Guard officials said that they saw little sharing of the intelligence at that level.

While we have not yet had the opportunity to observe the intelligence arms of TSA and the Coast Guard in action to more fully evaluate the potential for duplication of effort, it does appear that some potential duplication exists. From conversations with TSA and Coast Guard officials, we could discern little difference in a number of their information and integration efforts. Aside from potential inefficient use of resources, this possible duplication may also limit either agency from obtaining a complete intelligence picture and detecting potential threats.

Differences between Current TSA Grant Program and MTSA Grant Requirements

The final issue involves TSA's implementation of MTSA's grant program. MTSA required the Secretary of Transportation to establish a program of grants to ports and other entities to implement area and facility-specific security plans. Prior to the enactment of MTSA, TSA, in partnership with MARAD and the Coast Guard, already had begun a port security grant program in February 2002. This program was originally intended to fund security assessments and enhanced operational security at ports and facilities, and two rounds of grants were funded before MTSA was enacted in November 2002. TSA officials told us that, rather than creating a new grant program to specifically respond to MTSA, they are adapting the existing program to meet MTSA requirements. Under this approach, some time will elapse before all of the grant requirements specified under MTSA are in place.

The existing grant program differs from MTSA requirements in several respects. Most significantly, the existing grant program does not require cost-sharing, while MTSA does. MTSA grant provisions state that for projects costing more than $25,000, Federal funds for any eligible project shall not exceed 75 percent of the total cost. A TSA official said that, in starting to fold MTSA grants into the existing program for the third round of grants, TSA was still disbursing monies from a prior appropriation, and the language of that legislation limited its ability to make changes that would meet MTSA requirements. As a result, TSA encouraged cost-sharing but did not require it. While TSA limited its changes for the first three rounds of grants, in the future continued deviation from MTSA cost-sharing requirements would keep Federal dollars from reaching as many projects as possible. By not requiring a grantee to share in the financial burden, TSA does not take into account the applicant's ability to participate in the funding. If applicants have such

ability, the result is that available Federal dollars are not effectively leveraging as many projects as possible.[7]

There are two additional areas where TSA's current grant program differs from MTSA provisions. First, the current grant program does not specifically correspond to the stated purpose of MTSA's grant funding, which is to implement area and facility-specific security plans. TSA officials told us that in round three, they would give preference to regulated facilities and vessels that were already required to have security assessments and plans in place. As a result, the grants would likely be for mitigating identified vulnerabilities rather than developing plans. Second, in the application instructions for the current program, TSA said that recurring costs for personnel and operations and maintenance costs were not eligible for funding. MTSA specifically includes these costs.

TSA officials said that for later rounds of grants during Fiscal Year 2004, they would discuss potential changes in the Port Security Grant Program with the Coast Guard and MARAD. These potential changes would include requiring that all grant proposals be designed to meet MTSA port security grant requirements. The officials said, however, that before making any changes, they would look for specific directions accompanying currently pending appropriations for Fiscal Year 2004.

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

PREPARED STATEMENT OF GERALD L. DILLINGHAM, DIRECTOR, CIVIL AVIATION ISSUES, UNITED STATES GENERAL ACCOUNTING OFFICE

PROGRESS SINCE SEPTEMBER 11, 2001, AND THE CHALLENGES AHEAD

Mr. Chairman and Members of the Committee:

In the 2 years since the terrorist attacks of September 11, 2001, the security of our Nation's civil aviation system has assumed renewed urgency, and efforts to strengthen aviation security have received a great deal of congressional attention. On November 19, 2001, the Congress enacted the Aviation and Transportation Security Act (ATSA), which created the Transportation Security Administration (TSA) within the Department of Transportation (DOT) and defined its primary responsibility as ensuring security in aviation as well as in other modes of transportation. The act set forth specific improvements to aviation security for TSA to implement and established deadlines for completing many of them. The Homeland Security Act, passed on November 25, 2002, transferred TSA to the new Department of Homeland Security, which assumed overall responsibility for aviation security.

My testimony today addresses the (1) progress that has been made since September 11 to strengthen aviation security, (2) potential vulnerabilities that remain, and (3) longer-term management and organizational challenges to sustaining enhanced aviation security. The testimony is based on our prior work, our review of recent literature, and discussions with aviation industry representatives and TSA.

In summary:

Since September 2001, TSA has made considerable progress in meeting congressional mandates related to aviation security, thereby increasing aviation security. For example, by the end of December 2002, the agency had hired and deployed a workforce of about 65,000, including passenger and baggage screeners and Federal air marshals, and it was using explosives detection equipment to screen about 90 percent of all checked baggage. In addition, TSA has initiated several programs and research and development efforts that focus on the use of technology and information to advance security. For example, the agency is developing the Transportation Workers Identification Card program to provide a nationwide standard credential for airport workers that is issued after a background check has been completed and biometric indicators have been incorporated so that each worker can be positively matched to his or her credential. TSA is also developing the next-generation Computer Assisted Passenger Prescreening System (CAPPS II), which would use national security and commercial databases to assess the risk posed by passengers and identify some passengers for additional screening before they board their flights. These uses of technology and information—particularly CAPPS II—have raised some concerns about privacy rights that will need to be addressed as these programs move toward implementation.

---

[7] MTSA contains provisions for waiving the cost-sharing requirement if a higher level of Federal funding is required.

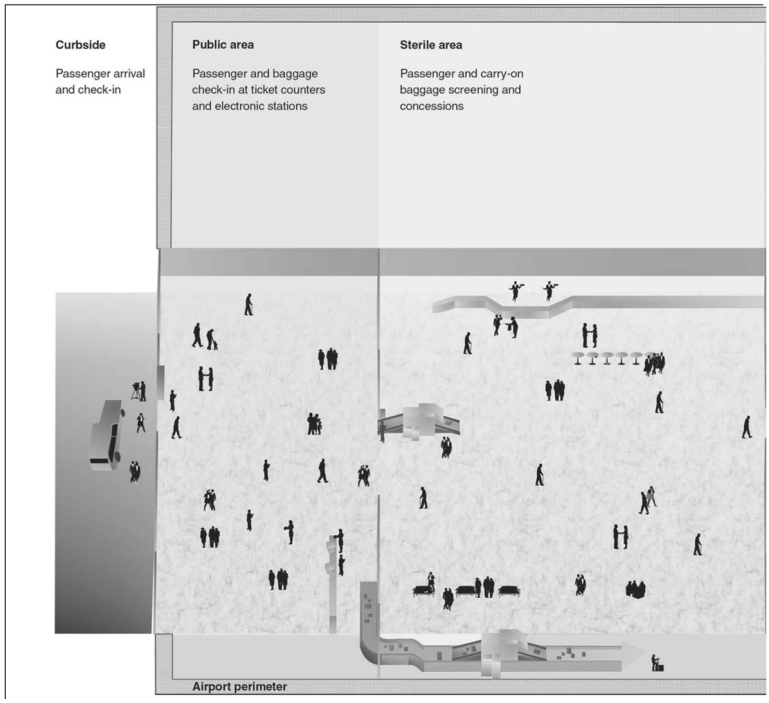
Although TSA has focused much effort and funding on ensuring that bombs and other threat items are not carried onto planes by passengers or in their luggage, vulnerabilities remain in areas such as air cargo security, general aviation security, and airport perimeter security. For example, air cargo is vulnerable because very little of the estimated 12.5 million tons transported each year on all-cargo and passenger planes is physically screened for explosives. As a result, a potential security risk is the introduction of explosive and incendiary devices in cargo placed aboard aircraft. We have recommended in prior work that TSA use a risk management approach to prioritize actions and funding as it works with industry to determine the next steps in strengthening air cargo security, and industry stakeholders have suggested the application of such an approach to general aviation security.

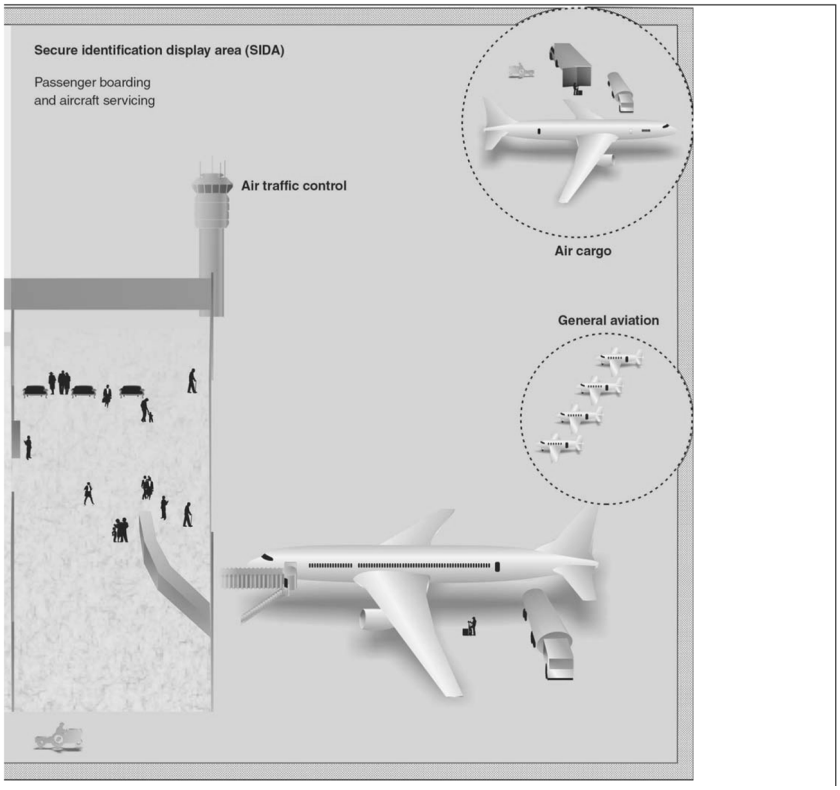
TSA faces longer-term management and organizational challenges to sustaining enhanced aviation security that include: (1) developing and implementing a comprehensive risk management approach, (2) paying for increased aviation security needs and controlling costs, (3) establishing effective coordination among the many public and private entities involved in aviation security, (4) strategically managing its workforce and ensuring appropriate staffing levels, and (5) building a results-oriented culture as it shifts its aviation security and other functions to the Department of Homeland Security. We have issued reports and made recommendations that address many of these challenges, and some actions are under way. In addition, we have studies in progress on some of these issues.

Background

Before September 2001, we and others had demonstrated significant, long-standing vulnerabilities in aviation security, some of which are depicted in figure 1. These included weaknesses in screening passengers and baggage, controlling access to secure areas at airports, and protecting air traffic control computer systems and facilities. To address these and other weaknesses, ATSA created the Transportation Security Administration and established security requirements for the new agency with mandated deadlines.

Figure 1: Aviation Security Focus Areas





Source: GAO.

Civil Aviation Was Vulnerable before September 11, 2001

Before September 2001, screeners, who were then hired by the airlines, often failed to detect threat objects located on passengers or in their carry-on luggage. Principal causes of screeners' performance problems were rapid turnover and insufficient training. As we previously reported, turnover rates exceeded 100 percent a year at most large airports, leaving few skilled and experienced screeners, primarily because of low wages, limited benefits, and repetitive, monotonous work.[1]

In addition, before September 2001, controls for limiting access to secure areas of airports, including aircraft, did not always work as intended. As we reported in May 2000, our special agents used fictitious law enforcement badges and credentials to gain access to secure areas, bypass security checkpoints at two airports, and walk unescorted to aircraft departure gates.[2] The agents, who had been issued tickets and boarding passes, could have carried weapons, explosives, or other dangerous objects onto aircraft. DOT's Inspector General also documented numerous problems with airport access controls, and in one series of tests, nearly 7 out of every 10 attempts by the Inspector General's staff to gain access to secure areas were successful. Upon entering the secure areas, the Inspector General's staff boarded aircraft 117 times. The Inspector General further reported that the majority of the aircraft

[1] U.S. General Accounting Office, *Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance,* GAO/RCED–00–75 (Washington, D.C.: June 28, 2000) and U.S. General Accounting Office, *Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security,* GAO–01–1166T (Washington, D.C.: Sept. 20, 2001).

[2] U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports,* GAO–OSI–0010 (Washington, D.C.: May 25, 2000).

boardings would not have occurred if employees had taken the prescribed steps, such as making sure doors closed behind them.

Our reviews also found that the security of the air traffic control computer systems and of the facilities that house them had not been ensured.[3] The vulnerabilities we identified, such as not ensuring that contractors who had access to the air traffic control computer systems had undergone background checks, made the air traffic control system susceptible to intrusion and malicious attacks. The air traffic control computer systems provide information to air traffic controllers and aircraft flight crews to help ensure the safe and expeditious movement of aircraft. Failure to protect these systems and their facilities could cause a nationwide disruption of air traffic or even collisions and loss of life.

Over the years, we made numerous recommendations to the Federal Aviation Administration (FAA), which, until ATSA's enactment, was responsible for aviation security. These recommendations were designed to improve screeners' performance, strengthen airport access controls, and better protect air traffic control computer systems and facilities. As of September 2001, FAA had implemented some of these recommendations and was addressing others, but its progress was often slow. In addition, many initiatives were not linked to specific deadlines, making it difficult to monitor and oversee their implementation.

Legislation Transferred Most Aviation Security Responsibilities to TSA

ATSA defined TSA's primary responsibility as ensuring security in all modes of transportation. The Act also shifted security-screening responsibilities from the airlines to TSA and established a series of requirements to strengthen aviation security, many of them with mandated implementation deadlines. For example, the act required the deployment of Federal screeners at 429 commercial airports across the Nation by November 19, 2002, and the use of explosives detection technology at these airports to screen every piece of checked baggage for explosives not later than December 31, 2002. However, the Homeland Security Act subsequently allowed TSA to grant waivers of up to 1 year to airports that would not be able to meet the December deadline.

Some aviation security responsibilities remained with FAA. For example, FAA is responsible for the security of its air traffic control and other computer systems and of its air traffic control facilities. FAA also administers the Airport Improvement Program (AIP) trust fund, which is used to fund capital improvements to airports, including some security enhancements, such as terminal modifications to accommodate explosives detection equipment.

Since September 2001, Multiple Initiatives Have Increased Aviation Security

Over the past 2 years, TSA and FAA have taken major steps to increase aviation security. TSA has implemented congressional mandates and explored options for increasing the use of technology and information to control access to secure areas of airports and to improve passenger screening. FAA has focused its efforts on enhancing the security of the Nation's air traffic control systems and facilities. In ongoing work, we are examining some of these efforts in more detail (see app. IV).

TSA Met Many Aviation Security Mandates but Encountered Some Difficulties

In its first year, TSA worked to establish its organization and focused primarily on meeting the aviation security deadlines set forth in ATSA, accomplishing a large number of tasks under a very ambitious schedule. In January 2002, TSA had 13 employees—1 year later, the agency had about 65,000 employees. TSA reported that it met over 30 deadlines during 2002 to improve aviation security. (See app. I for the status of mandates in ATSA.) For example, according to TSA, it:

- met the November 2002 deadline to deploy Federal passenger screeners at airports across the Nation by hiring, training, and deploying over 40,000 individuals to screen passengers at 429 commercial airports (see fig. 2);
- hired and deployed more than 20,000 individuals to screen all checked baggage;

[3] U.S. General Accounting Office, *Aviation Security: Weak Computer Security Practices Jeopardize Flight Safety,* GAO/AIMD–98–155 (Washington, D.C.: May 18, 1998); *Computer Security: FAA Needs to Improve Controls over Use of Foreign Nationals to Remediate and Review Software,* GAO/AIMD–00–55 (Washington, D.C.: Dec. 23, 1999); *Computer Security: FAA Is Addressing Personnel Weaknesses, but Further Action Is Required,* GAO/AIMD–00–169 (Washington, D.C.: May 31, 2000); *FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses,* GAO/AIMD–00–252 (Washington, D.C.: Aug. 16, 2000); and *FAA Computer Security: Recommendations to Address Continuing Weaknesses,* GAO–01–171 (Washington, D.C.: Dec. 6, 2000).

- has been using explosives detection systems or explosives trace detection equipment to screen about 90 percent of all checked baggage as of December 31, 2002;[4]
- has been using alternative means such as canine teams, hand searches, and passenger-bag matching to screen the remaining checked baggage;
- confiscated more than 4.8 million prohibited items (including firearms, knives, and incendiary or flammable objects) from passengers; and
- has made substantial progress in expanding the Federal Air Marshal Service.

In addition, according to FAA, U.S. and foreign airlines met the April 2003 deadline to harden cockpit doors on aircraft flying in the United States.

Figure 2: Screening Passengers at a U.S. Commercial Airport

Source: FAA.

Not unexpectedly, TSA experienced some difficulties in meeting these deadlines and achieving these goals. For example, operational and management control problems, cited later in this testimony, emerged with the rapid expansion of the Federal Air Marshal Service, and TSA's deployment of some explosives detection systems was delayed. As a result, TSA had to grant waivers of up to a year (until Dec. 31, 2003) to a few airports, authorizing them to use alternative means to screen all checked baggage. Recently, airport representatives with whom we spoke expressed concern that not all of these airports would meet the new December 2003 deadline established in their waivers because, according to the airport representatives, there has not been enough time to produce, install, and integrate all of the systems required to meet the deadline.

TSA Is Making Greater Use of Technology and Information to Enhance Aviation Security

To strengthen control over access to secure areas of airports and other transportation facilities, TSA is pursuing initiatives that make greater use of technology and information. For example, the agency is investigating the establishment of a Trans-

[4] Explosives detection machines are used to screen baggage for explosives and work by using CAT scan X-ray technology to take fundamental measurements of materials in bags to recognize characteristic signatures of threat explosives. Explosives trace detection systems (trace detection machines) are used to screen baggage for explosives, and work by detecting vapors and residues of explosives.

portation Workers Identification Card (TWIC) program. TWIC is intended to establish a uniform, nationwide standard for the secure identification of 12 million workers who require unescorted physical or cyber access to secure areas at airports and other transportation facilities. Specifically, TWIC will combine standard background checks and biometrics so that a worker can be positively matched to his or her credential. Once the program is fully operational, the TWIC card will be the standard credential for airport workers and will be accepted by all modes of transportation. According to TSA, developing a uniform, nationwide standard for identification will minimize redundant credentialing and background checks. Currently, each airport is required, as part of its security program, to issue credentials to workers who need access to secure, nonpublic areas, such as baggage loading areas.[5] Airport representatives have told us that they think a number of operational issues need to be resolved for the TWIC card to be feasible. For example, the TWIC card would have to be compatible with the many types of card readers used at airports around the country, or new card readers would have to be installed. At large airports, this could entail replacing hundreds of card readers, and airport representatives have expressed concerns about how this effort would be funded. In April 2003, TSA awarded a contract to test and evaluate various technologies at three pilot sites.

In addition, TSA has continued to develop the next-generation Computer Assisted Passenger Prescreening System (CAPPS II)—an automated passenger screening system that takes personal information, such as a passenger's name, date of birth, home address, and home telephone number, to confirm the passenger's identity and assess a risk level. The identifying information will be run against national security information and commercial databases, and a "risk" score will be assigned to the passenger. The risk score will determine any further screening that the passenger will undergo before boarding. TSA expects to implement CAPPS II throughout the United States by the fall of 2004. However, TSA's plans have raised concerns about travelers' privacy rights. It has been suggested, for example, that TSA is violating privacy laws by not explaining how the risk assessment data will be scored and used and how a TSA decision can be appealed. These concerns about the system will need to be addressed as it moves toward implementation. In ongoing work, we are examining CAPPS II, including how it will function, what safeguards will be put in place to protect the traveling public's privacy, and how the system will affect the traveling public in terms of costs, delays, and risks.

Additionally, TSA has begun to develop initiatives that could enable it to use its passenger screening resources more efficiently. For example, TSA has requested funding for Fiscal Year 2004 to begin developing a registered traveler program that would prescreen low-risk travelers. Under a registered traveler program, those who voluntarily apply to participate in the program and successfully pass background checks would receive a unique identifier or card that would enable them to be screened more quickly and would promote greater focus on those passengers who require more extensive screening at airport security checkpoints. In prior work, we identified key policy and implementation issues that would need to be resolved before a registered traveler program could be implemented. Such issues include the (1) criteria that should be established to determine eligibility to apply for the program, (2) kinds of background checks that should be used to certify applicants' eligibility to enroll in the program and the entity who should perform these checks, (3) security-screening procedures that registered travelers should undergo and the differences between these procedures and those for unregistered travelers, and (4) concerns that the traveling public or others may have about equity, privacy, and liability.[6]

FAA Is Strengthening Air Traffic Control Security

Since September 2001, FAA has continued to strengthen the security of the Nation's air traffic control computer systems and facilities in response to 39 recommendations we made between May 1998 and December 2000. For example, FAA has established an information systems security management structure under its Chief Information Officer, whose office has developed an information systems security strategy, security architecture (that is, an overall blueprint), security policies and directives, and a security awareness training campaign. This office has also managed FAA's incident response center and implemented a certification and accreditation process to ensure that vulnerabilities in current and future air traffic

[5] Under 49 C.F.R. sec. 1542.101, all qualified airports are required to have a TSA-approved security program that includes procedures to control movement within the secured area, including identification media required under sec. 1542.201(b)(3).

[6] U.S. General Accounting Office, *Aviation Security: Registered Traveler Program Policy and Implementation Issues,* GAO–03–253 (Washington, D.C.: Nov. 22, 2002).

control systems are identified and weaknesses addressed. Nevertheless, the office faces continued challenges in increasing its intrusion detection capabilities, obtaining accreditation for systems that are already operational, and managing information systems security throughout the agency. In addition, according to senior security officials, FAA has completed assessments of the physical security of its staffed facilities, but it has not yet accredited all of these air traffic control facilities as secure in compliance with its own policy. Finally, FAA has worked aggressively over the past 2 years to complete background investigations of numerous contractor employees. However, ensuring that all new contractors are assessed to determine which employees require background checks, and that those checks are completed in a timely manner, will be a continuing challenge for the agency.

Potential Vulnerabilities Remain in Several Aviation Sectors

Although TSA has focused much effort and funding on ensuring that bombs and other threat items are not carried onto commercial aircraft by passengers or in their luggage, vulnerabilities remain, according to aviation experts, TSA officials, and others. In particular, these vulnerabilities affect air cargo, general aviation, and airport perimeter security. For information on legislative proposals that would address these potential vulnerabilities and other aviation security issues, see appendix II.

Air Cargo Security

As we and DOT's Inspector General have reported, vulnerabilities exist in securing the cargo carried aboard commercial passenger and all-cargo aircraft. TSA has reported that an estimated 12.5 million tons of cargo are transported each year—9.7 million tons on all-cargo planes and 2.8 million tons on passenger planes. Some potential security risks associated with air cargo include the introduction of undetected explosive and incendiary devices in cargo placed aboard aircraft; the shipment of undeclared or undetected hazardous materials aboard aircraft; and aircraft hijackings and sabotage by individuals with access to cargo aircraft.[7] To address some of the risks associated with air cargo, ATSA requires that all cargo carried aboard commercial passenger aircraft be screened and that TSA have a system in place as soon as practicable to screen, inspect, or otherwise ensure the security of cargo on all-cargo aircraft. In August 2003, the Congressional Research Service reported that less than 5 percent of cargo placed on passenger airplanes is physically screened. TSA's primary approach to ensuring air cargo security and safety and to complying with the cargo-screening requirement in the act is the "known shipper" program—which allows shippers that have established business histories with air carriers or freight forwarders[8] to ship cargo on planes. However, we and DOT's Inspector General have identified weaknesses in the known shipper program and in TSA's procedures for approving freight forwarders.[9]

Since September 2001, TSA has taken a number of actions to enhance cargo security, such as implementing a database of known shippers in October 2002. The database is the first phase in developing a cargo-profiling system similar to the Computer-Assisted Passenger Prescreening System. However, in December 2002, we reported that additional operational and technological measures, such as checking the identity of individuals making cargo deliveries, have the potential to improve air cargo security in the near term.[10] We further reported that TSA lacks a comprehensive plan with long-term goals and performance targets for cargo security, time frames for completing security improvements, and risk-based criteria for prioritizing actions to achieve those goals. Accordingly, we recommended that TSA develop a comprehensive plan for air cargo security that incorporates a risk management approach, includes a list of security priorities, and sets deadlines for completing actions. TSA agreed with this recommendation and expects to develop such a plan by the fall of 2003. It will be important that this plan include a timetable for implementation and that TSA expeditiously reduce the vulnerabilities in this area.

---

[7] For example, on November 15, 1979, an explosive device contained in a parcel shipped by U.S. mail exploded aboard an American Airlines flight; on April 7, 1994, a Federal Express employee attempted to hijack a company plane and crash it into the company's headquarters. We reported on the security risks associated with dangerous goods in *Aviation Security: Vulnerability of Commercial Aviation to Attacks by Terrorists Using Dangerous Goods,* GAO–03–30C (Washington, D.C.: Dec. 3, 2002).

[8] Freight forwarders consolidate shipments and deliver them to air carriers and cargo facilities of passenger and all-cargo air carriers.

[9] U.S. General Accounting Office, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System,* GAO–03–344 (Washington, D.C.: Dec. 20, 2002).

[10] GAO–03–344.

General Aviation Security

Since September 2001, TSA has taken limited action to improve general aviation security, leaving it far more open and potentially vulnerable than commercial aviation.[11] General aviation is vulnerable because general aviation pilots are not screened before takeoff and the contents of general aviation planes are not screened at any point. General aviation includes more than 200,000 privately owned airplanes, which are located in every state at more than 19,000 airports. Over 550 of these airports also provide commercial service. In the last 5 years, about 70 aircraft have been stolen from general aviation airports, indicating a potential weakness that could be exploited by terrorists. Moreover, it was reported that the September 11 hijackers researched the use of crop dusters to spread biological or chemical agents. General aviation's vulnerability was revealed in January 2002, when a Florida teenage flight student crashed a single-engine Cessna airplane into a Tampa skyscraper.

FAA has since issued a notice with voluntary guidance for flight schools and businesses that provide services for aircraft and pilots at general aviation airports. The suggestions include using different keys to gain access to an aircraft and start the ignition, not giving students access to aircraft keys, ensuring positive identification of flight students, and training employees and pilots to report suspicious activities. However, because the guidance is voluntary, it is unknown how many general aviation airports have implemented these measures.

We reported in June 2003 that TSA was working with industry stakeholders as part of TSA's Aviation Security Advisory Council to close potential security gaps in general aviation.[12] According to our recent discussions with industry representatives, however, the stakeholders have not been able to reach a consensus on the actions needed to improve security in general aviation. General aviation industry representatives, such as the Aircraft Owners and Pilots Association and General Aviation Manufacturers Association, have opposed any restrictions on operating general aviation aircraft and believe that small planes do not pose a significant risk to the country. Nonetheless, some industry representatives indicated that the application of a risk management approach would be helpful in determining the next steps in improving general aviation security. (We discuss risk management in more detail later in this testimony.) To identify these next steps, TSA chartered a working group on general aviation within the existing Aviation Security Advisory Committee, and this working group is scheduled to report to the full committee in the fall of 2003. We have ongoing work that is examining general aviation security in further detail.

[11] For example, TSA issued a rule requiring that certain aircraft operators using aircraft with a maximum takeoff weight of 12,500 pounds or more carry out security measures, including conducting criminal history records checks on their flight crew members and restricting access to the flight deck. This rule went into effect in April 2003.

[12] U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges,* GAO–03–843 (Washington, D.C.: June 30, 2003).

Figure 3: General Aviation Aircraft and Airport

Source: Aircraft Owners and Pilots Association.

Airport Perimeter Security

Airport perimeters present a potential vulnerability by providing a route for individuals to gain unauthorized access to aircraft and secure areas of airports (see fig. 4). For example, in August 2003, the national media reported that three boaters wandered the tarmac at Kennedy International Airport after their boat became beached near a runway. In addition, terrorists could launch an attack using a shoulder-fired missile from the perimeter of an airport, as well as from locations just outside the perimeter. For example, in separate incidents in the late 1970s, guerrillas with shoulder-fired missiles shot down two Air Rhodesia planes. More recently, the national media have reported that since September 2001, al Qaeda has twice tried to down planes outside the United States with shoulder-fired missiles.[13]

We reported in June 2003 that airport operators have increased their patrols of airport perimeters since September 2001, but industry officials stated that they do not have enough resources to completely protect against missile attacks.[14] A number of technologies could be used to secure and monitor airport perimeters, including barriers, motion sensors, and closed-circuit television. Airport representatives have cautioned that as security enhancements are made to airport perimeters, it will be important for TSA to coordinate with FAA and the airport operators to ensure that any enhancements do not pose safety risks for aircraft. We have separate ongoing work examining the status of efforts to improve airport perimeter security and assessing the nature and extent of the threat from shoulder-fired missiles.

[13] The Department of Homeland Security is assessing proposals from eight contractors for technology to protect commercial aircraft from shoulder-fired missile attack.

[14] GAO–03–843.

Figure 4: Airport Perimeter

Source: GAO.

Aviation Security Poses Longer-Term Management and Organizational Challenges

TSA's efforts to strengthen and sustain aviation security face several longer-term challenges in the areas of risk management, funding, coordination, strategic human capital management, and building a results-oriented organization.

Risk Management

As aviation security is viewed in the larger context of transportation and homeland security, it will be important to set strategic priorities so that national resources can be directed to the greatest needs. Although TSA initially focused on increasing aviation security, it has more recently begun to address security in the other transportation modes. However, the size and diversity of the national transportation system make it difficult to adequately secure, and TSA and the Congress are faced with demands for additional Federal funding for transportation security that far exceed the additional amounts made available. We have advocated the use of a risk management approach to guide Federal programs and responses to better prepare for and withstand terrorist threats, and we have recommended that TSA use this approach to strengthen security in aviation as well as in other transportation modes.[15] A risk management approach is a systematic process to analyze threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions linking resources with prioritized efforts for results. Comprehensive risk-based assessments support effective planning and resource allocation. Figure 5 describes this approach.

[15] U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts,* GAO–02–208T (Washington, D.C.: Oct. 31, 2001); and GAO–03–344.

Figure 5: Elements of a Risk Management Approach

A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities. This assessment represents a systematic approach to identifying potential threats before they materialize. However, even if updated often, a threat assessment might not adequately capture some emerging threats. The risk management approach, therefore, uses vulnerability and criticality assessments as additional input to the decisionmaking process.

A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses.

A criticality assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy. The assessment provides a basis for identifying which structures or processes are relatively more important to protect from attack. As such, it helps managers to determine operational requirements and target resources at the highest priorities, while reducing the potential for targeting resources at lower priorities.

Source: GAO.

TSA agreed with our recommendation and has adopted a risk management approach in attempting to enhance security across all transportation modes. TSA's Office of Threat Assessment and Risk Management is developing two assessment tools that will help assess criticality, threats, and vulnerabilities. The first tool, which assesses criticality, will arrive at a criticality score for a facility or transportation asset by incorporating factors such as the number of fatalities that could occur during an attack and the economic and sociopolitical importance of the facility or asset. This score will enable TSA, in conjunction with transportation stakeholders, to rank facilities and assets within each mode and thus focus resources on those that are deemed most important. TSA is working with another Department of Homeland Security office—the Information Analysis and Infrastructure Protection Directorate—to ensure that the criticality tool will be consistent with the Department's overall approach for managing critical infrastructure.

The second tool—the Transportation Risk Assessment and Vulnerability Evaluation tool (TRAVEL)—will assess threats and analyze vulnerabilities for all transportation modes. The tool produces a relative risk score for potential attacks against a transportation asset or facility. In addition, TRAVEL will include a cost-benefit component that compares the cost of implementing a given countermeasure with the reduction in relative risk due to that countermeasure. We reported in June 2003 that TSA plans to use this tool to gather comparable threat and vulnerability information across all transportation modes. It is important for TSA to complete the development of the two tools and use them to prepare action plans for specific modes, such as aviation, and for transportation security generally.

Funding

Two key funding and accountability challenges will be (1) paying for increased aviation security and (2) ensuring that these costs are controlled. The costs associated with the equipment and personnel needed to screen passengers and their baggage alone are huge. The administration requested $4.2 billion for aviation security for Fiscal Year 2004, which included about $1.8 billion for passenger screening and $944 million for baggage screening.[16] ATSA created a passenger security fee to pay for the costs of aviation security, but the fee has not generated enough money to do so. DOT's Inspector General reported that the security fees are estimated to generate only about $1.7 billion in Fiscal Year 2004.[17]

A major funding issue is paying for the purchase and installation of the remaining explosives detection systems for the airports that received waivers, as well as for the reinstallation of the systems that were placed in airport lobbies last year and now need to be integrated into airport baggage-handling systems. Integrating the equipment with the baggage-handling systems is expected to be costly because it will require major facility modifications. For example, modifications needed to integrate the equipment at Boston's Logan International Airport are estimated to cost

[16] The House agreed to $3.7 billion in funding for TSA and the Senate approved $4.5 billion.

[17] TSA suspended the security fees from June 1 to September 30, 2003, as mandated by the Emergency Wartime Supplemental Appropriations Act of 2003.

$146 million. Estimates for Dallas/Fort Worth International Airport are $193 million. DOT's Inspector General has reported that the cost of integrating the equipment nationwide could be as high as $3 billion.

A key question is how to pay for these installation costs. Funds from FAA's AIP grants and passenger facility charges are eligible sources for funding this work.[18] In Fiscal Year 2002, AIP grant funds totaling $561 million were used for terminal modifications to enhance security. However, using these funds for security reduced the funding available for other airport development projects, such as projects to bring airports up to Federal design standards and reconstruction projects. In February 2003, we identified letters of intent[19] as a funding option that has been successfully used to leverage private sources of funding.[20] TSA has since signed letters of intent with three airports—Boston Logan, Dallas-Fort Worth, and Seattle-Tacoma International Airports. Under the agreements, TSA will pay 75 percent of the cost of integrating the explosives detection equipment into the baggage-handling systems. The payments will stretch out over 3 to 4 years. Airport representatives said that about 30 more airports have requested similar agreements. The slow pace of TSA's approval process has raised concerns about delays in reinstalling and integrating explosives detection equipment with baggage-handling systems—delays that will require more labor-intensive and less efficient baggage screening by other approved means.

To provide financial assistance to airports for security-related capital investments, such as the installation of explosives detection equipment, proposed aviation reauthorization legislation[21] would establish an aviation security capital fund that would authorize $2 billion over the next 4 years. The funding would be made available to airports in letters of intent, and large-and medium-hub airports would be expected to provide a match of 10 percent of a project's costs. A 5 percent match would be required for all other airports. This legislation would provide a dedicated source of funding for security-related capital investments and could minimize the need to use AIP funds for security.

An additional funding issue is how to ensure continued investment in transportation research and development. For Fiscal Year 2003, TSA was appropriated about $110 million for research and development, of which $75 million was designated for the next-generation explosives detection systems. However, TSA has proposed to reprogram $61.2 million of these funds to be used for other purposes, leaving about $12.7 million to be spent on research and development this year. This proposed reprogramming could limit TSA's ability to sustain and strengthen aviation security by continuing to invest in research and development for more effective equipment to screen passengers, their carry-on and checked baggage, and cargo. In ongoing work, we are examining the nature and scope of research and development work by TSA and the Department of Homeland Security, including their strategy for accelerating the development of transportation security technologies.

By reprogramming funds and making acknowledged use of certain funds for purposes other than those intended, TSA has raised congressional concerns about accountability. According to TSA, it has proposed to reprogram a total of $849.3 million during Fiscal Year 2003, including the $61.2 million that would be cut from research and development and $104 million that would be taken from the Federal air marshal program and used for unintended purposes. Because of these congressional concerns, we were asked to investigate TSA's process for reprogramming funds for the air marshal program and to assess the implications of the proposed funding reductions in areas such as the numbers of hours flown and flights taken. We have ongoing work to address these issues. To ensure appropriate oversight and accountability, it is important that TSA maintain clear and transparent communication with the Congress and industry stakeholders about the use of its funds.

In July 2002, we reported that long-term attention to cost and accountability controls for acquisition and related business processes will be critical for TSA, both to

---

[18] With FAA's approval, commercial airports may charge boarding passengers a fee of up to $4.50 per trip segment to raise funds for airport capital development.

[19] A letter of intent represents a nonbinding commitment from an agency to provide multiyear funding to an entity beyond the current authorization period. Thus, that letter allows an airport to proceed with a project without waiting for future Federal funds because the airport and investors know that allowable costs are likely to be reimbursed.

[20] U.S. General Accounting Office, *Airport Finance: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development,* GAO–03–497T (Washington, D.C.: Feb. 25, 2003).

[21] The proposed Vision 100—Century of Aviation Reauthorization—Act, H.R. 2115.

ensure its success and to maintain its integrity and accountability.[22] According to DOT's Inspector General, although TSA has made progress in addressing certain cost-related issues, it has not established an infrastructure that provides effective controls to monitor contractors' costs and performance.[23] For example, in February 2003, the Inspector General reported that TSA's $1 billion hiring effort cost more than most people expected and that TSA's contract with NCS Pearson to recruit, assess, and hire the screener workforce contained no safeguards to prevent cost increases. The Inspector General found that TSA provided limited oversight for the management of the contract expenses and, in one case, between $6 million and $9 million of the $18 million paid to a subcontractor appeared to be a result of wasteful and abusive spending practices.[24] As the Inspector General recommended, TSA has since hired the Defense Contract Audit Agency to audit its major contracts. To ensure control over TSA contracts, the Inspector General has further recommended that the Congress set aside a specific amount of TSA's contracting budget for overseeing contractors' performance with respect to cost, schedule, and quality.[25]

Coordination

Sustaining the aviation security advancements of the past 2 years also depends on TSA's ability to form effective partnerships with federal, state, and local agencies and with the aviation community. Effective, well-coordinated partnerships at the local level require identifying roles and responsibilities; developing effective, collaborative relationships with local and regional airports and emergency management and law enforcement agencies; agreeing on performance-based standards that describe desired outcomes; and sharing intelligence information. The lynchpin in TSA's efforts to coordinate with airports and local law enforcement and emergency response agencies is, according to the agency, the 158 Federal security directors and staff that TSA has deployed nationwide. The security directors' responsibilities include ensuring that standardized security procedures are implemented at the Nation's airports; working with state and local law enforcement personnel, when appropriate, to ensure airport and passenger security; and communicating threat information to airport operators and others. Airport representatives, however, have indicated that the relationships between Federal security directors and airport operators are still evolving and that better communication is needed at some airports.

Key to improving the coordination between TSA and local partners is establishing clearly defined roles. In some cases, concerns have arisen about conflicts between the roles of TSA, as the manager of security functions at airports, and of airport officials, as the managers of other airport operations. Industry representatives viewed such conflicts as leading to confusion in areas such as communicating with local entities. According to airport representatives, for example, TSA has developed guidance or rules for airports without involving them, and time-consuming changes have then had to be made to accommodate operational factors. The representatives maintain that it would be more efficient and effective to consider such operational factors earlier in the process. Ultimately, inadequate coordination and unclear roles result in inefficient uses of limited resources.

TSA also has to ensure that the terrorist and threat information gathered and maintained by law enforcement and other agencies—including the Federal Bureau of Investigation, the Immigration and Naturalization Service, the Central Intelligence Agency, and the Department of State—is quickly and efficiently communicated among Federal agencies and to state and local authorities, as needed. Disseminating such information is important to allow those who are involved in protecting the Nation's aviation system to address potential threats rather than simply react to known threats.

In aviation security, timely information sharing among agencies has been hampered by the agencies' reluctance to share sensitive information and by outdated, incompatible computer systems. As we found in reviewing 12 watch lists maintained by nine Federal agencies, information was being shared among some of them but not among others. Moreover, even when sharing was occurring, costly and overly complex measures had to be taken to facilitate it.[26] To promote better integration

---

[22] U.S. General Accounting Office, *Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges,* GAO–02–971T (Washington, D.C.: July 25, 2002).

[23] *Aviation Security Costs, Transportation Security Administration,* statement of the Honorable Kenneth M. Mead, Inspector General, U.S. Department of Transportation, before the Committee on Commerce, Science, and Transportation, Subcommittee on Aviation, U.S. Senate, Feb. 5, 2003 (CC–2003–066).

[24] DOT Inspector General, CC–2003–066.

[25] Office of Inspector General, DOT, *Report on Oversight of Security Screener Contracts, TSA,* FI–2003–025 (Washington, D.C.: Feb. 28, 2003).

[26] GAO–03–322.

and sharing of terrorist and criminal watch lists, we have recommended that the Department of Homeland Security, in collaboration with the other departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the Federal Government's watch list structures and policies.[27]

In addition, as we found earlier this year, representatives of numerous state and local governments and transportation industry associations indicated that the general threat warnings received by government agencies are not helpful. Rather, they said, transportation operators, including airport operators, want more specific intelligence information so that they can understand the true nature of a potential threat and implement appropriate security measures.[28]

Strategic Human Capital Management

As it organizes itself to protect the Nation's transportation system, TSA faces the challenge of strategically managing its workforce of more than 60,000 people, most of whom are deployed at airports or on aircraft to detect weapons and explosives and to prevent them from being taken aboard and used on aircraft. Additionally, over the next several years, TSA faces the challenge of "right-sizing" this workforce as efficiency is improved with new security-enhancing technologies, processes, and procedures. For example, as explosives detection systems are integrated with baggage-handling systems, the use of more labor-intensive screening methods, such as trace detection techniques and manual searches of baggage, can be reduced. Other planned security enhancements, such as CAPPS II and the registered traveler program, also have the potential to make screening more efficient.

To assist agencies in managing their human capital more strategically, we have developed a model that identifies cornerstones and related critical success factors that agencies should apply and steps they can take.[29] Our model is designed to help agency leaders effectively lead and manage their people and integrate human capital considerations into daily decision-making and the program results they seek to achieve.

In January 2003, we reported that TSA was addressing some critical human capital success factors by hiring personnel, using a wide range of tools available for hiring, and beginning to link individual performance to organizational goals.[30] However, concerns remain about the size and training of that workforce, the adequacy of the initial background checks for screeners, and TSA's progress in setting up a performance management system. As noted earlier in this testimony, TSA now plans to reduce its screener workforce by 6,000 by September 30, 2003, and it has proposed cutting the workforce by an additional 3,000 in Fiscal Year 2004. This planned reduction has raised concerns about passenger delays at airports and has led TSA to begin hiring part-time screeners to make more flexible and efficient use of its workforce. In addition, TSA used an abbreviated background check process to hire and deploy enough screeners to meet ATSA's screening deadlines in 2002. After obtaining additional background information, TSA terminated the employment of some of these screeners. TSA reported 1,208 terminations as of May 31, 2003, that it ascribed to a variety of reasons, including criminal offenses and failures to pass alcohol and drug tests. Furthermore, the national media have reported allegations of operational and management control problems that emerged with the expansion of the Federal Air Marshal Service, including inadequate background checks and training, uneven scheduling, and inadequate policies and procedures. In ongoing work, we are examining the effectiveness of TSA's efforts to train, equip, and supervise passenger screeners, and we are assessing the effects of expansion on the Federal Air Marshal Service. In addition, we reported in January 2003 that TSA had taken the initial steps in establishing a performance management system linked to organizational goals. Such a system will be critical for TSA to motivate and manage staff, ensure the quality of screeners' performance, and, ultimately, restore public confidence in air travel.

Building a Results-Oriented Organization

For TSA to sustain enhanced aviation security over the long term, it will be important for the agency to continue to build a results-oriented culture within the new Department of Homeland Security. To help Federal agencies successfully transform

---

[27] U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing,* GAO–03–322 (Washington, D.C.: Apr. 15, 2003).

[28] GAO–03–843.

[29] U.S. General Accounting Office, *A Model of Strategic Human Capital Management,* GAO–02–373SP (Washington, D.C.: March 2002).

[30] U.S. General Accounting Office, *Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture,* GAO–03–190 (Washington, D.C.: Jan. 13, 2003).

their cultures, as well as the new Department of Homeland Security merge its various components into a unified department, we identified key practices that have consistently been found at the center of successful mergers, acquisitions, and transformations.[31] These key practices, together with implementation strategies such as establishing a coherent mission and integrated strategic goals to guide the transformation, can help agencies become more results oriented, customer focused, and collaborative. (See app. III.) These practices are particularly important for the Department of Homeland Security, whose implementation and transformation we have designated as high risk.[32]

The Congress required TSA to adopt a results-oriented strategic planning and reporting framework and, specifically, to provide an action plan with goals and milestones to outline how acceptable levels of performance for aviation security would be achieved. In prior work, we reported that TSA has taken the first steps in performance planning and reporting by defining its mission, vision, and values and that this practice would continue to be important when TSA moved into the Department of Homeland Security.[33] Therefore, we recommended that TSA take the next steps to implement results-oriented practices. These steps included establishing performance goals and measures for all modes of transportation as part of a strategic planning process that involves stakeholders, defining more clearly the roles and responsibilities of its various offices in collaborating and communicating with stakeholders; and formalizing the roles and responsibilities of governmental entities for transportation security. Table 1 shows selected ATSA requirements, TSA's actions and plans, and the next steps we recommended. TSA agreed with our recommendations.

Table 1.—Requirements, Actions and Plans, and Recommended Next Steps for Results-Oriented Practices

ATSA requirements	TSA actions and plans	Next steps
Leadership commitment to creating a high-performing organization		
• Requires performance agreement between the Secretary of DOT and the Under Secretary of Transportation for Security and between the Under Secretary and TSA executives.	• Stated leadership commitment to creating a results-oriented culture in its 180-day action plan. • Expressed plans to use the Baldrige performance excellence criteria as a management tool to promote quality and performance. • Established standardized performance agreements for TSA executives.	• Establish a performance agreement for the Under Secretary of Transportation for Security that articulates how bonuses will be tied to performance. • Add expectations in performance agreements for top leadership to foster the culture of a high-performing organization.
Strategic planning to establish results-oriented goals and measures		
• Requires a 5-year performance plan and annual performance report consistent with the principles of the Government Performance and Results Act.	• Articulated vision, mission, values, strategic goal, and performance goals and measures. • Developed automated system to collect performance data to demonstrate progress in meeting goals. • Aligned aviation security performance goals and measures with DOT goals. • Reported it submitted first annual performance report.	• Establish security performance goals and measures for all modes of transportation as part of a strategic planning process that involves stakeholders. • Apply practices that have been shown to provide useful information in agency performance plans.
Performance management to promote accountability for results		
• Requires a performance management system. • Requires performance agreements for all employees that include organizational and individual goals.	• Established an interim performance management system. • Created standardized performance agreements for groups of employees that include organizational and individual goals and standards of performance.	• Build on the current performance agreements to achieve additional benefits. • Ensure the permanent performance management system makes meaningful distinctions in performance. • Involve employees in developing its permanent performance management system.

[31] U.S. General Accounting Office, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations,* GAO–03–669 (Washington, D.C.: July 2, 2003).

[32] U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security,* GAO–03–102 (Washington, D.C.: Jan. 1, 2003).

[33] GAO–03–190.

Table 1.—Requirements, Actions and Plans, and Recommended Next Steps for Results-Oriented Practices—Continued

ATSA requirements	TSA actions and plans	Next steps
Collaboration and communication to achieve national outcomes		
• Requires TSA to work within and outside the government to accomplish its mission. • Establishes a Transportation Security Oversight Board to facilitate collaboration and communication.	• Established Offices of Security Regulation and Policy, Communications and Public Information, Law Enforcement and Security Liaison, and Legislative Affairs to collaborate and communicate with stakeholders. • Convened the Oversight Board, which has met twice. • Stated plans to use memorandums of understanding and memorandums of agreement to formalize roles and responsibilities of TSA and other agencies in transportation security.	• Define more clearly the collaboration and communication roles and responsibilities of TSA's various offices. • Formalize roles and responsibilities among governmental entities for transportation security.
Public reporting and customer service to build citizen confidence		
• Requires a 180-day action plan and two progress reports within 6 months of enactment.	• Submitted 180-day action plan and both progress reports within established time frames. • Maintains a Website to provide information to the public. • Created ombudsman position to serve customers. • Developed measures to track customer satisfaction. • Reviewed and eliminated security procedures that do not enhance security or customer service. • Stated plans to develop a customer satisfaction index to analyze customer opinions to improve performance.	• Fill the ombudsman position to facilitate responsiveness of TSA to the public. • Continue to develop and implement mechanisms, such as the CSI, to gauge customer satisfaction and improve customer service.

Source: GAO.

Concluding Observations

After spending billions of dollars over the past 2 years on people, policies, and procedures to improve aviation security, we have much more security now than we had before September 2001, but it has not been determined how much more secure we are. The vast number of guns, knives, and other potential threat items that screeners have confiscated suggests that security is working, but it also suggests that improved public awareness of prohibited items could help focus resources where they are most needed and reduce delays and inconvenience to the public. Faced with vast and competing demands for security resources, TSA should continue its efforts to identify technologies, such as CAPPS II, that will leverage its resources and potentially improve its capabilities. Improving the efficiency and effectiveness of aviation security will also require risk assessments and plans that help maintain a balance between security and customer service.

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

APPENDIX I: SELECTED DEADLINES IN THE AVIATION AND TRANSPORTATION SECURITY ACT AND THEIR STATUS

Deadline	Provisions[a]	Status
Nov. 19, 2001	Require new background checks for those who have access to secure areas of the airport.	Completed
	Institute a 45-day waiting period for aliens seeking flight training for planes of 12,500 pounds or more.	Completed
Dec. 19, 2001	Establish qualifications for Federal screeners.	Completed
	Report to the Congress on improving general aviation security.	Completed
Jan. 18, 2002	Screen all checked baggage in U.S. airports using explosives detection systems, passenger-bag matching, manual searches, canine units, or other approved means.	Completed
	The Federal Aviation Administration (FAA) is to develop guidance for air carriers to use in developing programs to train flight and cabin crews to resist threats (within 60 days after FAA issues the guidance, each airline is to develop a training program and submit it to FAA; within 30 days of receiving a program, FAA is to approve it or require revisions; within 180 days of receiving FAA's approval, the airline is to complete the training of all flight and cabin crews).	Guidance issued
	Develop a plan to train Federal screeners.	Completed
	Foreign and domestic carriers are to provide electronic passenger and crew manifests to Customs for flights from foreign countries to the United States.	Completed
	Begin collecting the passenger security fee.	Completed
Feb. 17, 2002	The Under Secretary is to assume civil aviation security functions from FAA.	Completed
	Implement an aviation security program for charter carriers.	Completed
	Begin awarding grants for security-related research and development.	Completed
	The National Institute of Justice is to report to the Secretary on less-than-lethal weapons for flight crew members.	Completed
May 18, 2002	Report to the Congress on the deployment of baggage screening equipment.	Report submitted
	• Report to the Congress on progress in evaluating and taking the following optional actions:	Report submitted
	• Require 911 capability for onboard passenger telephones.	• Completed
	• Establish uniform IDs for law enforcement personnel carrying weapons on planes or in secure areas.	• Ongoing
	• Establish requirements for trusted traveler programs.	• Ongoing
	• Develop alternative security procedures to avoid damage to medical products.	• Completed
	• Provide for the use of secure communications technologies to inform airport security forces about passengers who are identified on security databases.	• Ongoing
	• Require pilot licenses to include a photograph and biometric identifiers.	• Ongoing
	• Use voice stress analysis, biometric, or other technologies to prevent high-risk passengers from boarding.	• Ongoing
	• Provide for the use of instant communications technology between planes and ground.	• Ongoing
Nov. 19, 2002	Deploy Federal screeners, security managers, and law enforcement officers to screen passengers and property.	Completed
	Report to the Congress on screening for small aircraft with 60 or fewer seats.	Report submitted
	Establish pilot program to contract with private screening companies (program to last until Nov. 19, 2004).	Completed
Dec. 31, 2002	Screen all checked baggage by explosives detection systems.	Ongoing
No deadline	Carriers are to transfer screening property to TSA.	Completed
	FAA is to issue an order prohibiting access to the flight deck, requiring strengthened cabin doors, requiring that cabin doors remain locked, and prohibiting possession of a key for all but the flight deck crew.	Completed
	Improve perimeter screening of all individuals, goods, property, and vehicles.	Ongoing
	Screen all cargo on passenger flights and cargo-only flights.	Ongoing
	Establish procedures for notifying FAA, state and local law enforcement officers, and airport security of known threats.	Completed

Deadline	Provisions[a]	Status
	Establish procedures for airlines to identify passengers who pose a potential security threat.	Ongoing
	FAA is to develop and implement methods for using cabin video monitors, continuously operating transponders, and notifying flight deck crew of a hijacking.	Ongoing
	Require flight training schools to conduct security awareness programs for employees.	Completed
	Work with airport operators to strengthen access control points and consider deploying technology to improve security access.	Ongoing
	Provide operational testing for screeners.	Ongoing
	Assess dual-use items that seem harmless but could be dangerous and inform screening personnel.	Ongoing
	Establish a system for measuring staff performance.	Ongoing
	Establish management accountability for meeting performance goals.	Ongoing
	Periodically review threats to civil aviation, including chemical and biological weapons.	Ongoing

Source: TSA.
[a]Except where otherwise indicated, the Transportation Security Administration (TSA) is responsible for implementing the provisions.

APPENDIX II: BILLS RELATED TO AVIATION SECURITY

H.R. 2144—Aviation Security Technical Corrections and Improvements Act—Many of the important provisions of this bill have been incorporated into the Conference Report version of the FAA Reauthorization Act, H.R. 2115.

S. 1409—Rebuild America Act of 2003—Establishes a new grant program in the Department of Homeland Security (DHS) for airport security improvements, including projects to replace baggage conveyer systems and projects to reconfigure terminal baggage areas as needed to install explosives detection systems. The Under Secretary for Border and Transportation Security is authorized to issue letters of intent to airports for these types of projects. One billion dollars is authorized for this program.

H.R. 2555—House and Senate versions of the Department of Homeland Security Appropriations Act for 2004 House version—Makes Fiscal Year 2004 appropriations of $3.679 billion for the Transportation Security Administration (TSA) to provide civil aviation security services (aviation security, Federal air marshals, maritime and land security, intelligence, research and development, and administration):

- $1.673 billion for passenger screening activities,
- $1.285 billion for baggage screening activities,
- $721 million for airport support and enforcement presence,
- $235 million for physical modifications of airports to provide for the installation of checked baggage explosives detection systems, and
- $100 million for the procurement of the explosives detection systems.

Continues to cap the number of screeners at 45,000 full-time equivalent positions.

Prohibits the use of funds authorized in this Act to pursue or adopt regulations requiring airport sponsors to provide, without cost to TSA, building construction, maintenance, utilities and expenses, or space for services relating to aviation security (excluding space for necessary checkpoints).

Senate Version of H.R. 2555—Makes Fiscal Year 2004 appropriations of $4.524 billion for TSA to provide civil aviation security services:

- $3.185 billion for screening activities,
- $1.339 billion for airport support and enforcement presence,
- $309 million for physical modifications of airports to provide for the installation of checked baggage explosives detection systems, and
- $151 million for the procurement of the explosives detection systems.

Prohibits the use of funds authorized in this Act to pursue or adopt regulations requiring airport sponsors to provide, without cost to TSA, building construction, maintenance, utilities and expenses, or space for services relating to aviation security (excluding space for necessary checkpoints).

Prohibits the use of funds authorized in this Act for the Computer Assisted Passenger Prescreening System (CAPPS II) until GAO has reported to the Committees on Appropriations that certain requirements have been met, including (1) the existence of a system of due process by which passengers considered to pose a threat may appeal their delay or prohibition from boarding a flight; (2) that the underlying

error rate of databases will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted; (3) that TSA has stressed-tested and demonstrated the efficacy and predictive accuracy of all search tools in CAPPS II; and (4) that the Secretary has established an internal oversight board to monitor the manner in which CAPPS II is being developed and prepared.

Requires a report from the Secretary of Homeland Security on actions taken to develop countermeasures for commercial aircraft against shoulder-fired missile systems and vulnerability assessments of this threat for larger airports.

H.R. 2115—Flight 100—Century of Aviation Reauthorization Act—Conference Report version—Gives FAA the authority to take a certificate action if it is notified by DHS that the holder of the certificate presents a security threat.

Gives the Secretary of Transportation the authority to make grants to general aviation entities (including airports, operators, and manufacturers) to reimburse them for security costs incurred and revenues lost because of restrictions imposed by the Federal Government in response to the events of September 11. The bill authorizes $100 million for these grants.

Authorizes DHS to reimburse air carriers and airports for all security screening activities they are still performing, such as for providing catering services and checking documents at security checkpoints and for providing the space and facilities used to perform screening functions to the extent funds are available.

Requires air carriers to carry out a training program for flight and cabin crews to prepare for possible threat conditions. TSA is required to establish minimum standards for this training within 1 year of the Act's passage.

Requires DHS to report in 6 months on the effectiveness of aviation security, specifically including the air marshal program; hardening of cockpit doors; and security screening of passengers, checked baggage, and cargo.

Establishes within DHS a grant program to airport sponsors for (1) projects to replace baggage conveyer systems related to aviation security; (2) projects to reconfigure terminal baggage areas as needed to install explosives detection systems; and (3) projects to enable the Under Secretary for Border and Transportation Security to deploy explosives detection systems behind the ticket counter, in the baggage sorting area, or in line with the baggage handling system. Requires $250 million annually from the existing aviation security fee that is paid by airline passengers to be deposited in an Aviation Security Capital Fund and made available to finance this grant program.

Requires TSA to certify that civil liberty and privacy issues have been addressed before implementing CAPPS II and requires GAO to assess TSA's compliance 3 months after TSA makes the required certification.

Allows cargo pilots to carry guns under the same program for pilots of passenger airlines. Permits an off-duty pilot to transport the gun in a lockbox in the passenger cabin rather than in the baggage hold. Also provides that both passenger and cargo pilots should be treated equitably in their access to training.

Requires security audits of all foreign repair stations within 18 months after TSA issues rules governing the audits. The rules must be issued within 240 days of enactment.

Requires background checks on aliens seeking flight training in aircraft regardless of the size of the aircraft. For all training on small aircraft, includes a notification requirement but no waiting period. For training on larger aircraft, adopts an expedited procedure if the applicant already has training, a license, or a background check, and adopts a 30-day waiting period for first-time training on large aircraft. Makes TSA responsible for the background check. Requires TSA to issue an interim final rule in 60 days to implement this section. This section takes effect when that rule becomes effective.

S.236—Background Checks for Foreign Flight School Applicants—Amends Federal aviation law to require a background check of alien flight school applicants without regard to the maximum certificated weight of the aircraft for which they seek training. (Currently, a background check is required for flight crews operating aircraft with a maximum certificated takeoff weight of 12,500 pounds or more.)

S. 165—Air Cargo Security Act—House companion bill (H.R. 1103)—Amends Federal aviation law to require the screening of cargo that is to be transported in passenger aircraft operated by domestic and foreign air carriers in interstate air transportation. Directs TSA to develop a strategic plan to carry out such screening. Requires the establishment of systems that (1) provide for the regular inspection of shipping facilities for cargo shipments; (2) provide an industrywide pilot program database of known shippers of cargo; (3) train persons that handle air cargo to ensure that such cargo is properly handled and safeguarded from security breaches; and (4) require air carriers operating all-cargo aircraft to have an approved plan for

the security of their air operations area, the cargo placed aboard the aircraft, and persons having access to their aircraft on the ground or in flight.

H.R. 1366—Aviation Industry Stabilization Act—Requires the Under Secretary for Border and Transportation Security, after all cockpit doors are strengthened, to consider and report to the Congress on whether it is necessary to require Federal air marshals to be seated in the first class cabin of an aircraft with strengthened cockpit doors.

Requires the Under Secretary to (1) undertake action necessary to improve the screening of mail so that it can be carried on passenger flights and (2) reimburse air carriers for certain screening and related activities, as well as the cost of fortifying cockpit doors, and for any financial losses attributed to the loss of air traffic resulting from the use of force against Iraq in calendar year 2003.

Establishes an air cargo security working group composed of various groups to develop recommendations on the enhancement of the current known shipper program.

H. R. 115—Aviation Biometric Badge Act—Amends Federal aviation law to direct TSA to require by regulation that each security screener (or employee who has unescorted access, or may permit other individuals to have unescorted access, to an aircraft or a secured area of the airport) be issued a biometric security badge that identifies a person by fingerprint or retinal recognition.

H. R. 1049—Arming Cargo Pilots Against Terrorism Act—Senate companion bill (S. 516)—Expresses the sense of Congress that a flight deck crew member of a cargo aircraft should be armed with a firearm to defend such aircraft against attacks by terrorists that could use the aircraft as a weapon of mass destruction or for other terrorist purposes. Amends Federal transportation law to authorize the training and arming of flight deck crew members (pilots) of all-cargo air transportation flights to prevent acts of criminal violence or air piracy.

H.R. 765—(No title)—Legislation to arm cargo pilots—Amends Federal aviation law to allow cargo pilots (not just air passenger pilots) to participate in the Federal flight deck officer program.

H.R. 580—Commercial Airline Missile Defense Act—Senate companion bill—S. 311—Directs the Secretary of Transportation to issue regulations that require all turbojet aircraft of air carriers to be equipped with a missile defense system. Requires the Secretary to purchase such defense systems and make them available to all air carriers. Sets forth certain interim security measures to be taken before the deployment of such defense systems.

APPENDIX III: KEY PRACTICES AND IMPLEMENTATION STEPS FOR MERGERS AND ORGANIZATIONAL TRANSFORMATIONS

Practice	Implementation step
Ensure top leadership drives the transformation.	• Define and articulate a succinct and compelling reason for change. • Balance continued delivery of services with merger and transformation activities.
Establish a coherent mission and integrated strategic goals to guide the transformation.	• Adopt leading practices for results-oriented strategic planning and reporting.
Focus on a key set of principles and priorities at the outset of the transformation.	• Embed core values in every aspect of the organization to reinforce the new culture.
Set implementation goals and a time line to build momentum and show progress from day one.	• Make public implementation goals and a time line. • Seek and monitor employee attitudes and take appropriate follow-up actions. • Identify cultural features of merging organizations to increase understanding of former work environments. • Attract and retain key talent. • Establish an organizationwide knowledge and skills inventory to exchange knowledge among merging organizations.
Dedicate an implementation team to manage the transformation process.	• Establish networks to support the implementation team. • Select high-performing team members.
Use the performance management system to define responsibility and ensure accountability for change.	• Adopt leading practices to implement effective performance management systems with adequate safeguards.

Practice	Implementation step
Establish a communication strategy to create shared expectations and report related progress.	• Communicate early and often to build trust. • Ensure consistency of message. • Encourage two-way communication. • Provide information to meet specific needs of employees.
Involve employees to obtain their ideas and gain their ownership for the transformation.	• Use employee teams. • Involve employees in planning and sharing performance information. • Incorporate employee feedback into new policies and procedures. • Delegate authority to appropriate organizational levels.
Build a world-class organization.	• Adopt leading practices to build a world-class organization.

Source: GAO.

APPENDIX IV: GAO ACTIVE ENGAGEMENTS RELATED TO AVIATION SECURITY

Transportation Security Research and Development Programs at DHS and TSA

Key Questions: (1) What were the strategy and organizational structure for transportation security research and development (R&D) prior to 9/11 and what is the current strategy and structure? (2) How do DHS and TSA select their transportation security R&D projects and what projects are in their portfolios? (3) What are DHS's and TSA's goals and strategies for accelerating the development of transportation security technologies? (4) What are the nature and scope of coordination of R&D efforts between DHS and TSA, as well as with other public and private sector research organizations?

Federal Air Marshal Service

Key Questions: (1) How has the Federal air marshal program evolved, in terms of recruiting, training, retention, and operations since its management was transferred to TSA? (2) To what extent has TSA implemented the internal controls needed to meet the program's operational and management control challenges? (3) To what extent has TSA developed plans and initiatives to sustain the program and accommodate its future growth and maturation?

TSA Baggage Screening

Key Questions: (1) What are the status and associated costs of TSA's efforts to acquire, install, and operate explosives detection equipment (electronic trace detection technology and explosives detection systems) to screen all checked baggage by December 31, 2003? (2) What are the benefits and trade-offs—to include costs, operations, and performance—of using alternative explosives detection technologies currently available for baggage screening?

Reprogramming of Air Marshal Program Funds

Key Questions: (1) Describe the internal preparation, review, and approval process for DHS's reprogrammings and, specifically, the process for the May 15 and July 25 reprogramming requests for the air marshal program. (2) Determine whether an impoundment or deferral notice should have been sent to the Congress and any other associated legal issues. (3) Identify the implications, for both the air marshal program and other programs, of the pending reprogramming request.

General Aviation Security

Key Questions: (1) How have security concerns and measures changed at general aviation airports since September 11, 2001? (2) What steps has TSA taken to improve general aviation security?

Background Checks for Banner-Towing Aircraft

Key Questions: (1) What are the procedures for conducting background and security checks for pilots of small banner-towing aircraft requesting waivers to perform stadium overflights? (2) To what extent have these procedures been followed in conducting required background and security checks since September 11, 2001? (3) How effective have these procedures been in reducing risks to public safety?

TSA's Computer Assisted Passenger Prescreening System II (CAPPS II)

Key Questions: (1) How will the CAPPS II system function and what data will be needed to make the system operationally effective? (2) What safeguards will be put in place to protect the traveling public's privacy? (3) What systems and measures are in place to determine whether CAPPS II will result in improved national secu-

rity? (4) What impact will CAPPS II have on the traveling public and on the airline industry in terms of costs, delays, risks, inconvenience, and other factors?

TSA Passengers Screening Program

Key Questions: (1) What efforts have been taken or planned to ensure that passenger screeners comply with Federal standards and other criteria, including efforts to train, equip, and supervise passenger screeners? (2) What methods does TSA use to test screeners' performance, and what have been the results of these tests? (3) How have the results of tests of TSA passenger screeners compared with the results achieved by screeners before September 11, 2001, and at five pilot program airports? (4) What actions is TSA taking to remedy performance concerns?

TSA's Efforts to Implement Sections 106, 136, and 138 of the Aviation and Transportation Security Act

Key Questions: What is the status of TSA's efforts to implement (1) section 106 of the act requiring improved airport perimeter access security, (2) section 136 requiring the assessment and deployment of commercially available security practices and technologies, and (3) section 138 requiring background investigations for TSA and other airport employees?

Assessment of the Portable Air Defense Missile Threat

Key Questions: (1) What are the nature and extent of the threat from man-portable air defense systems (MANPAD)? (2) How effective are U.S. controls on the use of exported MANPADs? (3) How do multilateral efforts attempt to stem MANPAD proliferation? (4) What types of countermeasures are available to minimize this threat and at what cost?

Airline Assistance Determination of Whether the $5 Billion Provided by P.L. 107–42 Was Used to Compensate the Nation's Major Air Carriers for Their Losses Stemming from the Events of Sept. 11, 2001

Key Questions: (1) Was the $5 billion used only to compensate major air carriers for their uninsured losses incurred as a result of the terrorist attacks? (2) Were carriers reimbursed, per the act, only for increases in insurance premiums resulting from the attacks?

TSA's Use of Sole-Source Contracts

Key Questions: (1) To what extent does TSA follow applicable acquisition laws and policies, including those for ensuring adequate competition? (2) How well does TSA's organizational structure facilitate effective, efficient procurement? (3) How does TSA ensure that its acquisition workforce is equipped to award and oversee contracts? (4) How well do TSA's policies and processes ensure that TSA receives the supplies and services it needs on time and at reasonable cost?

RELATED GAO PRODUCTS

Aviation Security

Transportation Security: Federal Action Needed to Help Address Security Challenges. GAO–03–843. Washington, D.C.: June 30, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO–03–616T. Washington, D.C.: April 1, 2003.

Aviation Security: Measures Needed to Improve Security of Pilot Certification Process. GAO–03–248NI. Washington, D.C.: February 3, 2003. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO–03–286NI. Washington, D.C.: December 20, 2002. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO–03–344. Washington, D.C.: December 20, 2002.

Aviation Security: Vulnerability of Commercial Aviation to Attacks by Terrorists Using Dangerous Goods. GAO–03–30C. Washington, D.C.: December 3, 2002.

Aviation Security: Registered Traveler Program Policy and Implementation Issues. GAO–03–253. Washington, D.C.: November 22, 2002.

Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges. GAO–02–971T. Washington, D.C.: July 25, 2002.

Aviation Security: Information Concerning the Arming of Commercial Pilots. GAO–02–822R. Washington, D.C.: June 28, 2002.

Aviation Security: Deployment and Capabilities of Explosive Detection Equipment. GAO–02–713C. Washington, D.C.: June 20, 2002. (CLASSIFIED)

Aviation Security: Information on Vulnerabilities in the Nation's Air Transportation System. GAO–01–1164T. Washington, D.C.: September 26, 2001. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Information on the Nation's Air Transportation System Vulnerabilities. GAO–01–1174T. Washington, D.C.: September 26, 2001. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Vulnerabilities in, and Alternatives for, Preboard Screening Security Operations. GAO–01–1171T. Washington, D.C.: September 25, 2001.

Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities. GAO–01–1165T. Washington, D.C.: September 21, 2001.

Aviation Security: Terrorist Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports. GAO–01–1162T. Washington, D.C.: September 20, 2001.

Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security. GAO–01–1166T. Washington, D.C.: September 20, 2001.

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO–01–1069R. Washington, D.C.: August 31, 2001.

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO–01–1068R. Washington, D.C.: August 31, 2001. (RESTRICTED)

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO–01–171. Washington, D.C.: December 6, 2000.

Aviation Security: Additional Controls Needed to Address Weaknesses in Carriage of Weapons Regulations. GAO/RCED–00–181. Washington, D.C.: September 29, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. GAO/T–AIMD–00–330. Washington, D.C.: September 27, 2000.

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses. GAO/AIMD–00–252. Washington, D.C.: August 16, 2000.

Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance. GAO/RCED–00–75. Washington, D.C.: June 28, 2000.

Aviation Security: Screeners Continue to Have Serious Problems Detecting Dangerous Objects. GAO/RCED–00–159. Washington, D.C.: June 22, 2000. (NOT FOR PUBLIC DISSEMINATION)

Computer Security: FAA Is Addressing Personnel Weaknesses, but Further Action Is Required. GAO/AIMD–00–169. Washington, D.C.: May 31, 2000.

Security: Breaches at Federal Agencies and Airports. GAO–OSI–00–10. Washington, D.C.: May 25, 2000.

Aviation Security: Screener Performance in Detecting Dangerous Objects during FAA Testing Is Not Adequate. GAO/T–RCED–00–143. Washington, D.C.: April 6, 2000. (NOT FOR PUBLIC DISSEMINATION)

Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism. GAO/NSIAD–00–85. Washington, D.C.: April 7, 2000.

Aviation Security: Vulnerabilities Still Exist in the Aviation Security System. GAO/T–RCED/AIMD–00–142. Washington, D.C.: April 6, 2000.

U.S. Customs Service: Better Targeting of Airline Passengers for Personal Searches Could Produce Better Results. GAO/GGD–00–38. Washington, D.C.: March 17, 2000.

Aviation Security: Screeners Not Adequately Detecting Threat Objects during FAA Testing. GAO/T–RCED–00–124. Washington, D.C.: March 16, 2000. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Slow Progress in Addressing Long-Standing Screener Performance Problems. GAO/T–RCED–00–125. Washington, D.C.: March 16, 2000.

Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software. GAO/AIMD–00–55. Washington, D.C.: December 23, 1999.

Aviation Security: FAA's Actions to Study Responsibilities and Funding for Airport Security and to Certify Screening Companies. GAO/RCED–199–53. Washington, D.C.: February 24, 1999.

Aviation Security: FAA's Deployments of Equipment to Detect Traces of Explosives. GAO/RCED–99–32R. Washington, D.C.: November 13, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. GAO/AIMD–98–155. Washington, D.C.: May 18, 1998.

Aviation Security: Progress Being Made, but Long-Term Attention Is Needed. GAO/T–RCED–98–190. Washington, D.C.: May 14, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. GAO/AIMD–98–60. Washington, D.C.: April 29, 1998. (LIMITED OFFICIAL USE –DO NOT DISSEMINATE)

Aviation Security: Implementation of Recommendations Is Under Way, but Completion Will Take Several Years. GAO/RCED–98–102. Washington, D.C.: April 24, 1998.

Combating Terrorism: Observations on Crosscutting Issues. T–NSIAD–98–164. Washington, D.C.: April 23, 1998.

Aviation Safety: Weaknesses in Inspection and Enforcement Limit FAA in Identifying and Responding to Risks. GAO/RCED–98–6. Washington, D.C.: February 27, 1998.

Aviation Security: FAA's Procurement of Explosives Detection Devices. GAO/RCED–97–111R. Washington, D.C.: May 1, 1997.

Aviation Security: Commercially Available Advanced Explosives Detection Devices. GAO/RCED–97-ll9R. Washington, D.C.: April 24, 1997.

Aviation Safety and Security: Challenges to Implementing the Recommendations of the White House Commission on Aviation Safety and Security. GAO/T–RCED–97–90. Washington, D.C.: March 5, 1997.

Aviation Security: Technology's Role in Addressing Vulnerabilities. GAO/T–RCED/NSIAD–96–262. Washington, D.C.: September 19, 1996.

Aviation Security: Oversight of Initiatives Will Be Needed. C–GAO/T–RCED/NSIAD–96–20. Washington, D.C.: September 17, 1996. (CLASSIFIED)

Aviation Security: Urgent Issues Need to Be Addressed. GAO/T–RCED/NSIAD–96–251. Washington, D.C.: September 11, 1996.

Aviation Security: Immediate Action Needed to Improve Security. GAO/T–RCED/NSIAD–96–237. Washington, D.C.: August 1, 1996.

Aviation Security: FAA Can Help Ensure That Airports' Access Control Systems Are Cost Effective. GAO/RCED–95–25. Washington, D.C.: March 1, 1995.

Aviation Security: Development of New Security Technology Has Not Met Expectations. GAO/RCED–94–142. Washington, D.C.: May 19, 1994.

Aviation Security: Additional Actions Needed to Meet Domestic and International Challenges. GAO/RCED–94–38. Washington, D.C.: January 27, 1994.

Other

Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues. GAO–03–715T. Washington, D.C.: May 3, 2003.

Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing. GAO–03–322. Washington, D.C.: April 15, 2003.

Combating Terrorism: Observations on National Strategies Related to Terrorism. GAO–03–519T. Washington, D.C.: March 3, 2003.

Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture. GAO–03–190. Washington, D.C.: January 17, 2003.

Major Management Challenges and Program Risks: Department of Homeland Security. GAO–03–102. Washington, D.C.: January 1, 2003.

Major Management Challenges and Program Risks: Department of Transportation. GAO–03–108. Washington, D.C.: January 2003.

National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security. GAO–02–621T. Washington, D.C.: April 11, 2002.

Homeland Security: Progress Made, More Direction and Partnership Sought. GAO–02–490T. Washington, D.C.: March 12, 2002.

A Model of Human Capital Management. GAO–02–373SP. Washington, D.C.: March 2002.

Senator LOTT. Under the early bird rule, Senator Hollings, you'll get the first shot at questions.

Senator HOLLINGS. Thank you, Mr. Chairman.

Most advisedly, I got here before we even had a Department of Transportation, and the country is very, very fortunate in having the team that we do have at the table here testifying this morning. This is the best working group I've ever seen on the transportation needs of the country.

Having said that, let me get right to the money part, because, Admiral Collins, again on Sunday, and then now in the morning [*Washington Post*] paper, business section, you have the Coast Guard doing an outstanding job—there's no question about it—but shortchanged on money. You see, you can come up and ask for $87 billion for some other place, over in Iraq, but you can't ask for the money here, because OMB has got you fellows all lockjawed. This is your one chance to get it. That's our problem here. And the military has a bad habit of saluting and going forward, rather than, by God, raising the question. If Secretary Powell had not saluted and raised some questions and stuck with them, we wouldn't be in that quagmire.

But, having said that, Admiral Collins, where do you get, now, the automated identification system? I find that the oil tankers and the cruise ships have transponders, I guess. We don't have the towers up yet, do we?

Admiral COLLINS. No, Senator, we do not. The infrastructure—that particular infrastructure is not in place. The two approaches to that, a short-term approach, is to embed AIS in all our vessel traffic service systems, the existing infrastructure there, and that's unfolding and will be completed through and into 2005. The longer-term effort is to build an infrastructure around our entire coast that can take those signals.

Senator HOLLINGS. Well, we've taken care of overall needs there. You had a $7.2 billion needs projection. And how much of that have you received and how much do you need?

Admiral COLLINS. The figures on $1.5 and over $7 billion of the cost estimates associated with the implementation of the Maritime Transportation Security Act, and those would—that would be the costs, the estimated costs, that the private sector would bear in implementing the terms and conditions of that act. It would be $1.5 billion the first year, and over $7 billion over 10 years. That would be all the efforts they would need to conduct assessment, develop plans, structure exercises, and make associated investments in their infrastructure relative to security needs. So that's the——

Senator HOLLINGS. Has the Committee approved all you need? You've got all you need?

Admiral COLLINS. We think that the support of the budget 2004 budget, the President's budget, would be a great benefit to the United States Coast Guard and maritime security. We have over a 10 percent——

Senator HOLLINGS. I know it's going to be a great benefit. Do you have all you need?

Admiral COLLINS. I guess you could say you'd never had all you——

Senator HOLLINGS. Well, what——

Admiral COLLINS.—would desire. But I think that's a very significant—between the 2003 and the 2004 budget, we've realized a 30-percent increase in the budget, going to the United States Coast Guard—that's a significant increase, and we'll——

Senator HOLLINGS. Admiral, most advisedly, I know it's an increase, but I've been listening for years on end that you're underfunded, and you have been underfunded. Senator Lott, Senator Stevens, and myself are on the Appropriations Committee have to steal from 050 from the Defense Department to supplement you. And I can't ever get the testimony from you, other than, "Oh, it's a wonderful thing, and it's happy, and it's going to be a big help."

Anyway, let me move then to—since my time is limited here—Admiral Loy. Again, you're doing a magnificent job, you and Commissioner Bonner, working as a team. You say we have forged working partnerships. But the integrated system of maritime intelligence. Now Customs has pulled out, Coast Guard has opened up two new centers, and TSA is planning one of its own. I speak, again, from experience. Forty-nine years ago, I served on the Hoover Commission investigating Alan Dulles and J. Edgar Hoover and the intelligence activities. They didn't talk to each other. Tenet and Mueller now do talk to each other. But within your own department you all are going off on all directions, and you get that little lady from the National Security Agency hollering, "They didn't have anything specific. They didn't have anything specific," like the terrorist's going to call up on the phone and tell you they're going to hit the tower. You know what I mean?

[Laughter.]

Admiral LOY. Yes, sir.

Senator HOLLINGS. You've got to have these things coordinated and the dots joined, and you all are going in all different directions rather than forge working partnerships. How is it that Customs has pulled out, the Coast Guard has opened two new centers, and the TSA, you've got planning one intelligence entity of your own?

Admiral LOY. Sir, what we have in place is what we inherited from the FAA, in terms of an intelligence——

Senator HOLLINGS. But you're supposed to clean it up——

Admiral LOY. Yes, sir. I'm working hard——

Senator HOLLINGS.—and you all are supposed to work together.

Admiral LOY. I'm working hard to—doing that. There are a variety of requirements that Tom has, for example, at Coast Guard, with respect to counter-narcotics or fisheries enforcement that are not appropriate for an integrated center that's focused principally on the rest of maritime security. The Judge has things that he and I have in common, about cargo, for example, or passenger concerns, that perhaps aren't the responsibility of Tom.

My concern here is that the functional purpose of maritime security be dealt with, intelligencewise, in the manner you and I have talked about many times, and I think that's not a bricks-and-mortar kind of notion; it's a collaborative coordination kind of notion. And, at the moment, with a brand new department, with an organization being stood up known as TTIC, with lots of other things in the intelligence world going on, that sorting process has just not come to closure as to whether or not, for example, as the appropriation called for, that $25 million would come to TSA to build an intelligence cell——

Senator HOLLINGS. But as Mr. Guerrero just pointed out, you need a working agreement. You get on top of that, and rather than going all off and starting new intelligence endeavors, hither, thither, and yon, get all together one, because that was one of the big misgivings by the Congress itself, that Homeland Security did not include, of course, the intelligence efforts of the CIA and the FBI.

Admiral LOY. Yes, sir.

Senator HOLLINGS. And now if you all are going all different directions, the same thing that happened on 9/11 can happen again, even though you all knew about it.

Admiral LOY. Yes, sir. And I think the greatest opportunity for doing exactly that, Senator Hollings, is—now that Under Secretary Libutti is in his chair, he's responsible for that intelligence analysis and information-sharing piece of the new department, that will allow us all to centralize one place where we deal with what we're dealing with in the maritime——

Senator HOLLINGS. Thank you, Mr. Chairman.

Senator LOTT. Thank you, Senator Hollings, for your interest and involvement in this area for many, many years and for your always interesting, entertaining questions and comments.

Let me see here. Admiral Collins, in the past you have experimented with the aerostat balloon radars and other systems to provide your cutters with large area radar picture surface targets. You know, if that can be used at a reasonable cost, wouldn't it be worthwhile to pursue that kind of technology?

Admiral COLLINS. Clearly, we're, Senator, looking at ways to enhance what we—as I referred to, maritime domain awareness, and that's a visibility of what's happening in the maritime, and it's—there are a variety of systems and subsystems that are part of that—that can be and should be part of that architecture. For instance, vessel traffic systems in the radar NTVs and so forth are part of that system. Our integrated Deepwater system, which building out a fleet of cutters in UAVs is part of that, that's a subsystem of this larger awareness thing where we've done some development and demonstration of a high-frequency surface-wave radar in the Florida Keys to get a picture of moving traffic. And we have a demonstration project that I know that Senator Stevens is very, very interested in, and it's using UAVs in Alaska. So we're approaching this in a multifaceted way, looking at various sensor options that will give us the visibility that we need.

And I know that the United States Navy, NORTHCOM, and others are very, very interested in that national surveillance architecture, and that's what we really need. I don't think there's any one silver bullet, but we need a national maritime surveillance archi-

tecture. We don't have that now. And we're going to work very, very hard to create that picture.

I have just set up a program office within Coast Guard headquarters, which we call the Maritime Domain Awareness Program Office, to develop specifically that overarching architecture where all these systems would plug in and give us the integrated picture that we need.

Senator LOTT. All right. You mentioned the Deepwater Project. How is that coming? I mean, I know you've made some preliminary decisions, and you've got some companies that are working toward, you know, producing all this additional equipment you need——

Admiral COLLINS. Yes, sir.

Senator LOTT.—cutters and everything. And it has been, you know, budgeted by the Administration, but each year, we've had to move it up, and you're already beginning to fall behind.

Admiral COLLINS. Yes, sir. We——

Senator LOTT. We need to try to make up some ground this year. Would you give us a specific report on that?

Admiral COLLINS. Yes, sir. Of course, we awarded that contract last June, I think, a very, very positive or—in a strategic partnership with—Northrop Grumman and Lockheed Martin are the joint-venture folks orchestrating that, the integrators. A lot of progress in the ship-design task order for initial engineering and development of the two Casa aircraft that are a part of that program, and more to follow—110 patrol boats going into Lockport and Bollinger Shipyards to get stretched into 123 vessels and some improvements in the C4ISRs, a lot of movement, a lot of very, very good progress.

One of the issues, of course, is the capital cash flow associated with this project and how—and we are, as you noted, a little behind the initial design that said that to get to a 20- to 25-year program, which is the long program, that you'd need, at minimum, $500 million a year in 1998 dollars to meet that timeline. At the present clip, we're about—and I think there are verified by GAO as a number—we're $202 million behind that timeline through 2004, and I know both the House and the Senate have increased the President's request for Deepwater in recognition of that hole in the road, so to speak, that we have.

Senator LOTT. All right. We'll keep pushing that to try to be helpful, but I do think that the success of this program will depend, to a large degree, on how closely you manage it and stay on top of it now. And so I hope you will continue to do that.

Admiral Loy, I mentioned, in my opening statement, you know, my concern about AIP funds going for security costs. And, obviously, the Committee and Congress has indicated a desire not for that to continue. Would you like to comment on that? If you're not going to get AIP funds, are you, you know, getting what you do need for airport security from other accounts?

Admiral LOY. Sir, to get back to the Senator's number that he used in his opening statement, I think you used a $5 billion estimate that may have come out of the GAO reports, as well as other places. Yes, sir.

First of all, with respect to AIP, it was an enormously valuable jumpstart kind of notion that in the interest of the airports and all of us across the country sharing in the burden of jumpstarting

aviation security, AIP funds in 2002 and 2003 were used in the fashion you described. We have no intention of continuing to depend on AIP money, which is there for another purpose, and we understand that to be the case. The greatest boost that allows us to not go there any longer, Senator Lott is the recognition by the Congress and by the Administration that letters of intent, the same kind of tool used in the AIP structure, can be used literally out of our own appropriation to fund some of these challenges that continue to exist across the country.

Senator Hollings' number of $5 billion, I would offer that comes probably more from the airport directors and their summation than from what I'd call a bit more objective read. The DOT IG's read in that regard is somewhere between $2 billion and $3 billion to deal with the cleanup process, if you will. We, as an organization, when we installed this EDS equipment across the country, left a bit of a wake behind us in a number of different places. This estimate is between $2 billionand $3 billion to go and clean that up. So far, we have issued, as you know, sir, six letters of intent to major airports in the country—adds up to about $670 million over the course of the next four or five budget cycles. But the good thing is there—it's not all capital up front; it's a reimbursable kind of a process, like AIP.

Senator LOTT. Well, now, let me—I guess this is a statement more than a question, but I would hope that you would apply common sense in the things that you direct the airports to do. Some of the things I have been made familiar with that you've requested or ordered don't make common sense, like reinforce that entrance wall of a small remote airport. I mean, a terrorist couldn't find the place, let alone blow the wall up. And also be careful about taking over local law enforcement stuff. When you tell an airport that you've got to do more about security in the parking area that's away from the terminal, if I were the local people, I'd tell you, "OK, you pay for it, because we're not going to do what you dictate to us. We don't think it makes common sense." I just hope we would use some common sense and practicalities, and remember that these people, local people, have to come up with these costs from somewhere and—tell you no, unless you can justify it or come up with the money.

And I do think, in a lot of areas, you've gobbled up a lot of space that really is not necessary. You know, maybe you needed it at the beginning, but you need to go back and evaluate that. Those airports have other uses for that space.

I don't know how many pilots you've really trained, but I understand it's only about a hundred. A year ago, I urged you to use some of the same people that train our Special Forces, our Delta Force, our—oh, the guys—well, the Special Forces, let's leave it there. You didn't—that's done in the private sector. You said, "Oh, no, we'll do it." It hasn't worked very well. I would urge you to go back and let the same people that trained the SEALs and the Special Forces, you know, train these pilots. It, you know, would take about 2 weeks, maybe. And you've trained about a—I don't know, maybe a hundred in a year.

One final point. On the ports and security ports, the size of the port is not as important as the threat, what's coming into that port.

If you just do it on the basis of size, I mean, you just come to the biggest port right on down. But if you have a port, for instance, that's got—right close to the mouth of the channel, national security components, Coast Guard cutters, oil refineries, that would be a more dangerous port than one that might be bigger located in another area. So be careful not to neglect some of the medium- or smaller-sized ports that have a higher risk prospect.

Admiral LOY. Sir, if I could comment just once—on one or two of those notions.

The last one, I could not agree with you more. The approach is to weigh very carefully, together with the Coast Guard and all the other players that are a part of those decisions, is this an out-load port, is this an economically important port, is this a port that deals precisely with taking the opportunity to think through the kind of things that you're mentioning.

And I think you're going, sir, toward the ultimate notion of port security grants and being able to make sure that we're not just exclusively giving them out to the largest ports, based on the thinking pattern that you just described. That's precisely the kind of weighted algorithm, if you will, that we're using to make those decisions.

As it relates to FFDO, sir, the Federal Flight Deck Officer Program, we will probably have about 500 trained by the end of this month. We have used every nickel that was provided to us in that program to do that training this year. We have $25 million in the President's request and, I think, surviving in both the Senate and the House mark for next year, which will train every volunteer that has identified themselves as being interested in the program. So the Federal Flight Deck Officer Program is on track. It is a high-quality program that we can all be proud of.

Senator LOTT. Thank you very much.

Senator Lautenberg?

Senator LAUTENBERG. Thanks, Mr. Chairman.

I think it's fair to say that we've got a very distinguished group of leaders here, and we appreciate the difficulty of the task that you've taken. But I also commend you on your policy to swallow hard and go forward, because there are all kinds of questions raised about whether or not we sacrifice something out of Customs in order to take care of security, and what does that mean by way of tax collections, cargo inspections, et cetera. And I'll try to ask my questions quickly so we can get quick answers and I don't run too much—I know the red lights permit continuing conversation, but——

Something Senator Lott just said struck me, and he comes from a port state or a coastal state, as I do, and that is the high-threat areas. Now, what better evidence do we need of a high threat than the attack on the Trade Centers? What better example do we need of a high-threat area than to look at the volume of traffic that goes through the Port of New York/New Jersey? What better example do we need of a high-threat area when you have all of these airplanes coming into three major airports plus a couple of relatively smaller ones? So I think when we talk about delineating dollars for the right places, we have to look at the New York/New Jersey area. And I'll tell you, on the formula for distribution that we've got, we

are really left out in the pasture, and it's not fair and it's not sensible not to go ahead and reexamine the allocation of the funds for security.

Admiral Loy and Admiral Collins, we're all friends of the Coast Guard. I very much appreciated what you did. And Senator Hollings is a fan of the Coast Guard, as well. And we always wondered—because we served in Appropriations together in my former life here, and you were always getting new tasks, always getting new assignments, whether it was pollution control or illegal immigrants or manifests or navigation aids, you name it, and we kept on reducing the size of the budget, and I never could quite understand how you did it, Admiral Loy, in your day, and now Admiral Collins. And I see things as small as rubber boats, inflatables, with a couple of Coast Guard's people going up and down the Hudson River helping to keep our ports safe.

So I would—you know, I don't want you to come here and crow about what you don't have. You've taken it with a semi-smile, Admiral Collins, but I'd like to sneak in there and find out what you really think about your budget.

[Laughter.]

Senator LAUTENBERG. But I want to ask, Admiral Loy, Commissioner Bonner, my colleagues introduced legislation to protect aircraft against SAM attacks, but it would take a few years to upgrade all the airliners with proper anti-SAM technology. What do we do now, beside worry? And I don't ever mean to trivialize your efforts. What, realistically, can we do to protect the perimeters of our airports?

Admiral LOY. Let me take a first stab at it, sir. First of all, we have instituted a pretty aggressive assessment program for all of the major airports. We're done with the category-X airports, well through the inventory of category-1 airports, and have focused, as well, on those 17 airports, that are foreign, from which most high-profile aircraft are coming to the United States. So the notion of those places where U.S. carriers are operating most of the time carrying heavy loads of people from place to place, the assessment effort is what I'd call one of the three legs of this stool of attack on the MANPADS issue on the shoulder-fired weapons issue. And that is about tactical countermeasures. What kind of things can we do in a tactical countermeasures sense to do a better job than has been done in the past?

In the wake of those assessments, an engagement effort with the local Federal Security director and his team or her team, with local law enforcement, with state law enforcement, has been engaged at each one of those major airports, with the view that we would be identifying logical places where such a missile could be launched, and dealing as constructively as we can with either perimeter security associated with it, with lighting, with fencing, with cameras, with roving patrols, or whatever might be appropriate that that local team takes on. That's one piece.

The second piece is about nonproliferation. In other words, in the same vein that we have been concerned about international nonproliferation of any kind of a weapons system, we want to be as aggressive with respect to that in MANPADS as we can possibly be. That is, we've all heard numbers of how many hundreds of

thousands of these things are actually in inventory around the world. Inducing the international community to hold onto that inventory, to identify where each and every one of them is, and deal with manufacturing and distribution things that are under the control of major government forces, whether it's buyback programs, whether it's destruction programs. That second——

Senator LAUTENBERG. Admiral Loy, I hate to interrupt, but I must, only because if we tell the public-at-large that we're going to inventory the four or five hundred thousand of these things, et cetera, et cetera, it's not really comforting. And I'm not criticizing you. The magnitude of the problem that we're dealing with here is something almost beyond comprehension, because if we look at the SAM program and then, taking Mr. Guerrero's report from GAO where he says according to TSA solutions that can be implemented relatively easily at the Nation's commercial airports are not practical at 19,000 general aviation airports. And I use a lot of the general aviation.

Now, it would be awful if one of our airplanes or another nation's airplanes was struck by a missile, but somebody can get into a single-engine plane, and if they carry enough explosive in that airplane to go down to one of our nuclear plants and decide that suicide is the way for them to go, we are practically helpless to guard against that. The one thing that I would hope is, maybe a system can be introduced at these general aviation airports that says you can't even takeoff—provided there's a manager there; a lot of these places don't have a manager, rely on the pilot to light the runway lights, but if there is a manager there—is to demand that any flight that takes off has some kind of a log that they have to fill, or be introduced to a human being, at least you know who's getting out there. It's a very complicated——

Admiral LOY. That's exactly the direction we're going with respect to the GA community, sir, with respect to background investigations on players that are always at the airport, local knowledge of who's getting in that airplane, tie-downs required when—you know, just so that any terrorist can't go and find that aircraft, get in it, and take it where he wants to go.

To close the MANPADS thing, sir, the most important leg is the technical countermeasures piece, which is what Ms. Boxer's bill is about, which is what your concern is about. That is probably, in my estimation, clearly one of the most important projects being undertaken by the combination of DOD and DHS to come to closure on what we're going to do with technical countermeasures.

Mr. BONNER. Can I just add one thing, Senator, just very briefly?

Senator LAUTENBERG. Sure.

Mr. BONNER. There's no one solution, but another thing you want to do here is to prevent those terrorists that might get that general aviation airplane or the terrorist who might bring a terrorist weapon into the United States, like a SAM–7 or a MANPAD, and you want to do everything we can to be able to identify and detect that when it's being brought into the country. And we have systems, we've increased our staffing to do that, and we use a targeted system to identify both the high-risk people and the high-risk shipments into the country. So it's just another layer of things that we're doing to prevent a MANPAD attack.

Senator LAUTENBERG. Mr. Chairman, I'll conclude, because the red light is on, and usually in traffic that means speed up.

[Laughter.]

Senator LAUTENBERG. What I would like to ask here is, the Department——

Well, you see it—don't get in the crossroad too early——

[Laughter.]

Senator LAUTENBERG. The Department of Homeland Security has proposed, even as we labor to make this program ever more effective, cutting the port security grant program by $105 million. In the interest of security, I have to raise the question about why, at the three major airports—that's Newark, JFK, and La Guardia—they reduced the Federal complement of law enforcement personnel from 64 to 19. I mean, that's kind of going backward. Why are the—did the Air Marshal Program wind up as a target for cuts, and suddenly there was a reverse field here that said, "Now, wait a second. We're going to take other people from other departments and train them as air marshals." Is there no price to the other departments when we grab people from one and put them in another, when we train them to be air marshals, when, in fact, they're Customs people, or otherwise?

Admiral LOY. Shall I take a shot at that, sir?

Senator LAUTENBERG. Please, somebody.

Admiral LOY. Sure. The shift of the Federal Air Marshal Program from TSA to BICE, the law enforcement gathered functional centralization effort that both Under Secretary Hutchinson and Secretary Ridge have decided to do, was a move that takes advantage of a number of things and I don't believe disadvantages TSA at the other end of the day, in terms of becoming, if you will, a demanding customer of BICE services about Federal air marshals, when heretofore we've been able to schedule them on our own.

I'll let the Judge or anyone else answer the question about surge capability, which is, in fact, what the Secretary has in mind. He is so concerned, as we all are, about the path of aviation-related intelligence things going by, that he wanted surge capability to be available to him if we felt that we needed more air marshals for whatever the short period of time might be. He feels that the relocation to the BICE bureau offers a chance for cross-training among Federal law enforcement officers that could potentially provide that surge, and, further, to get the Federal air marshals out of the absolute uniqueness of only going to the air and back on a daily basis, and offer career-path adjustments and opportunities for them elsewhere inside the BICE location.

So that's the thinking pattern behind why we sent the Federal air marshals to the BICE bureau.

Senator LOTT. Senator Snowe?

STATEMENT OF HON. OLYMPIA J. SNOWE,
U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman. I want to thank all of you for being here today.

Beginning with you, Admiral Loy, I know our director in Portland, Maine, testified during a Senate Governmental Affairs hearing recently that there is little or no coordination between the Fed-

eral Government and that his department comes to protecting the Port of Portland. In fact, he said, "We find ourselves in the unique position of acting as mediators between various rulemaking bodies. On my desk, I have a plethora of paper designed to help me secure the port. These rules cover everything from the height of fences to the height of lettering on badges. They're issued by agencies without regard or knowledge of what other agencies are regulating."

I understand we're obviously in a transitional phase here, but what can we do to have a better order and system involved among all the agencies with respect to the types of rules and regulations that are imposed on, in this case, in port directors and transportation directors? Because that is an issue and has been problematic, I know, in the past. But I think it is important to have some kind of consistency, some kind of organization where they can respond to, you know, one agency——

Admiral LOY. Absolutely.

Senator SNOWE.—one individual.

Admiral LOY. Absolutely. The notion of what kind of cross-modal oversight and responsibilities should be borne by a single agency in the Federal establishment, if you will, is part and parcel behind what TSA is supposed to be all about. That was the congressional intent, that was why the President signed the bill, and that's why we exist. So to the degree we can take and fill in the blanks on that Rubik's cube chart that I showed before, that is the intended purpose for all of that.

On the other hand, as it relates to a port I think it's quite clear that the Coast Guard is the lead Federal agency with respect to that kind of oversight. The captain of the port is the fellow, locally, that should represent, if you will, the aggregate interest of Federal requirements for that particular port across the country. The harbor safety committees, or whatever functional entity serves as a harbor safety committee in each and every port, usually has the captain of the port sitting at the head of the table able to make good consensus judgments from all the players that are there.

I'd be happy, by the way, to engage this particular gentleman or lady with respect to those issues you described and see what we can do to work that out.

Senator SNOWE. Right. He was recommending—and it would be interesting hearing from you, Admiral Collins, as well, about—he's proposing a representative of some of the critical non-Federal agencies in each port to have top security clearance so they can respond to the threats, as well.

Admiral LOY. Sure.

Senator SNOWE. Because who currently is aware of the types of threats that might exist in the ports and can receive that information? Is there anybody who's designated? Is it the port director? Who receives that information? I gather it's given from you, Admiral Collins.

Admiral COLLINS. Right. The port under MTSA, of course, the captain of the port, as Admiral Loy has indicated, is designated as the Federal Maritime Security Coordinator in the port and is the clearinghouse for that kind of information. And it's true, and I have great hopes and expectations for the port security committees that are required to be established under MTSA, chaired by each cap-

tain of the port, that they become that kind of clearinghouse, with very diverse representation from the port members, that decide those kind of things and become a clearinghouse of information in and through the port.

So I think, as we implement MTSA and the rulemaking, I think we're going to see some real positive coordination. There's going to be an overarching area security plan for the port, individual facility plans that each facility will do, vessel plans, and all integrated and reviewed at that port security committee, and that port security committee being the funnel for that information, up and down.

Incidentally, all those port security committees are, even though the bulk of the rule goes into effect 1 July of next summer, most of those port security committees around the country have been established, membership is being determined, and meetings are happening. So I think that—again, no one silver bullet to information exchange, but I think that is going to be a very, very positive development for information sharing.

Senator SNOWE. And when is——

Admiral LOY. On that, Senator Snowe, if I may——

Senator SNOWE. Yes.

Admiral LOY.—ma'am. You asked about classification. I think that's a legitimate issue. In the aviation environment, each of the airlines has a security director, properly cleared, that we can engage, as necessary, in passing information of a classified nature when we have it and when it's appropriate to be passed. That needs to be part of the scene at the port, as well. And MTSA notionalizes that in the construct Tom just described there should be a number of players with adequate clearances that can accept classified information and take care of the port in that regard.

Senator SNOWE. I appreciate that.

How would you grade the port security threat now, in terms of the fact that we have taken sufficient or insufficient mitigating steps at this point?

Admiral LOY. I think each of us probably has an answer to that, but first let me—I would say we are significantly better off than we were on the occasion of 9/11/01. The description of CSI and CTPAT, the kind programs that Judge Bonner has mentioned here with respect to pushing our borders out, that's a concept the three of us have bought into——

Senator SNOWE. Right.

Admiral LOY.—100 percent. The notions Tom was just describing on MTSA and how that's going to play out in the port, this is all a sort of step function on the way to where we want to be. We're certainly not there yet, but we're an awful lot better off than we were, with a good game plan in place to get where we need to be.

Senator SNOWE. I'm certainly—I know that Customs, Mr. Bonner, for example, has initiated their container security initiative in assigning 20 inspectors to foreign ports, but that seems like a very minuscule number considering the number of foreign ports that exist, and also requires the acquiescence and the approval of host countries to allow our inspectors on their docks to inspect the containers before they are loaded on, which obviously would be preferable, rather than waiting until those ships are coming to the United States.

Mr. BONNER. Well, we're at 16 foreign ports right now, so we have it operational. And the number is probably closer to about a hundred U.S. Customs and Border Protection personnel that are stationed overseas that are working with our host nation counterparts for the container security initiative.

It's important to realize what they're doing. They're principally—you know, they are principally over there to do the targeting and work with the host nation to identify particularly the high-risk containers for terrorism security issues. And then our host nation actually, in each and every instance, has agreed to go forward and do the security check of those containers, which is both for radiation detection and running them through large-scale X-ray type scanning machines to make sure that those containers do not pose a risk to U.S. seaports.

So we have implemented it. The surprising thing, Senator Snowe—and I don't know that it's so surprising—but the reality is that we started off targeting or identifying the 20 largest foreign seaports, in terms of the shipments of containers to the United States. We have agreements from the countries that represent 19 of those 20 to implement the container security initiative. And, as I said, we've actually now have expanded the number of agreements, and we—it's not just something we're talking about; it's something that we've actually implemented now in 16 foreign ports, and we're expanding. We'll have it up and operated in over 20 of the top foreign ports.

That's important, because just the top 20 foreign ports alone represent almost—over two thirds, almost 70 percent, of every cargo container that's shipped to the United States—and there's 7 million a year—originate from or are trans-shipped through just those 20 ports. So we've made great progress.

Now, the reason why is that those other countries are willing to do this because they recognize it's in their own interest to protect, essentially, the trade lanes between Rotterdam and U.S. ports, or from Singapore and U.S. ports, or for Yokohama, Hong Kong, Bremerhaven, and those places. They recognize it's in their interest to protect these shipping lanes. It also provides us with a protection for what is the primary system of global trade, which is containerized shipping to U.S. seaports.

So it's working very well, and there's a tremendous acceptance of this by other nations of the world, so far.

Senator SNOWE. And just one other issue, and I appreciate it.

Admiral Loy, pre-clearance at Canadian airports, is that something that you intend to address? That does concern me. Of the seven airports in Canada that have pre-clearance, and in Vancouver, they even have an in-transit pre-clearance, so that other—so that people can bypass Canadian Customs.

Admiral LOY. We pre-clear, actually——

Senator SNOWE. You do the pre-clearances.

Admiral LOY.—Senator Snowe. It's actually Customs and Border Protection, which is now both Customs and Immigration Inspectors.

We have a pre-clearance for both Customs and Immigration purposes at all of the seven largest international airports in Canada, so we actually do pre-clear there—actually in several other coun-

tries, as well. And that gives us an opportunity to identify people that pose a potential threat to the United States, identify them there, deny admissibility or take other appropriate law enforcement action with respect to those interviews—individuals. We have, right now—it's maybe 150, 160—no, it's probably—actually, with Customs and Immigration, probably closer to about 300 U.S. Customs and Border Protection Inspectors at the Canadian airports that pre-clear, both pre-screen and pre-clear, for Customs and Immigration purposes, at those airports.

Senator SNOWE. Well, given the recent report that came out regarding the huge gaps in the security systems in Canada, it raises those issues as to whether or not it's sufficient enough to ensure that anybody who poses a risk to our security enters the country—doesn't enter the country.

Admiral LOY. Well, I know, but we have a chance in Canada actually to stop them——

Senator SNOWE. OK.

Admiral LOY.—in Canada, rather than waiting for them to actually get on an airplane headed for the U.S., which actually gives us——

Senator SNOWE. They're all screened.

Admiral LOY. They are all screened.

Senator SNOWE. OK.

Admiral LOY. Each and every person is. And we also have advance information, so we're also doing some risk analysis with respect to people. But everybody is screened, and we have the right to question and to carry out searches of their luggage, both carry-on and checked luggage, before they leave—before they get on planes from Canada for the U.S.

Senator SNOWE. Thank you.

Senator LOTT. Senator Breaux?

STATEMENT OF HON. JOHN B. BREAUX,
U.S. SENATOR FROM LOUISIANA

Senator BREAUX. Let me thank the panel members. Every one of you are distinguished public servants. We've worked with you for a number of years.

Admiral Loy, you mentioned something early in your testimony about the weakest link and trying to find it. If I were looking for the weakest link in our security system in transportation, I'd look to the maritime ports, and I think I'd find it there.

The Administration has requested $87 billion for Afghanistan and for Iraq, partially for security purposes in that country. The Administration has requested zero for grants to the ports. And yet the legislation that we have passed have required the ports to do innumerable activities that are going to cost money. And I think that that is a huge hole that we have created, and a burden on the local ports. Aviation, I think, is in fairly good shape. We've got Federal officials running around all of the airports, and we've got screeners, we've got Federal officials. We don't have that type of system in the ports. There's a great deal that needs to be done. And, for the life of me, I cannot understand the justification for not a dollar, not a dime, being requested for new grants for the maritime ports. And every single one of them—and you've met with

them, and Admiral Collins has, and we all have—there's a huge need. And to come before the Congress and say zero dollars for grants to maritime ports is unacceptable. I think it is unconscionable as a matter of priorities, considering what we're doing in other parts of the world, which many of us will try and support.

But there's a great need here in this country. And I'm all for improving port security in Iraq, but I'm also for securing the Port of New Orleans and the Port of Los Angeles and the Port of New York. And we're not doing enough domestically in that area.

Can I have a comment from anybody about that, in terms of priorities?

Admiral LOY. Senator Breaux, yours is a voice that is very carefully listened to. I will carry that message back to the boss, as it relates to the request on the part of budgets as they are coming forward to the Congress. I will also recognize that over the course of the last two budget cycles, the Congress has recognized port security grants and bus grants and highway grants and other such things as being enormously important.

I think, sir, we're in this classic place we've been often in our country, where a tragedy happened, and it was immediately followed by a relatively emotional piece of legislation, or multiple pieces of legislation, and then 8 months later the sticker shock set in, in terms of sorting out what was needed to be done and what was the resource base necessary to do that. And in the case of TSA, of course, we didn't even have a base by which to make—you know, from which to make marginal adjustments. We literally had to create that.

That discussion is still, I think, going on and often takes—as it did, for example, when OPA 90 happened, in the aftermath of the Exxon Valdez hitting the rocks in Prince William Sound—it took us 10 years to sort out the regulatory regimes that were necessary to deal with that.

Senator BREAUX. Well, the sticker shock apparently has not set in on Iraq.

Admiral LOY. Sir.

Senator BREAUX. You've also requested on the Automatic Identification System, which we all felt was a good idea before 9/11, to know where these ships are coming from, who they are, what their cargo is. And we all agreed, even before 9/11, this is the right thing to do. We'd like to know where the ships are coming from, with greater detail of what's in the cargo, who's manning the ships, et cetera, why they're sitting out there. An Automatic Identification System would help us in that.

And, Admiral Collins, you talked about how the towers aren't there, and I note that the budget request is a million dollars. One million dollars, for the entire country for the Automatic Identification System, AIS. That is not going to get it done. That's not going to get you started, in a real significant way, in putting into play a system for the maritime ports to allow us to know where the ships are coming from. We know where the airplanes are coming from. We know where they're going. We track them constantly. But we're not doing that to the ships, and we're not going to have enough money for the ports to do what we are requiring them to do.

So if I was looking at the weakest link, it wouldn't be at the airports. If I was a terrorist, I certainly wouldn't want to try something that dealt with aviation, because of all the security we have on the ground, around the airports, on the airplanes, with marshals. We do not have anything comparable in the maritime ports of this country. It is a huge problem. And if it's a huge problem, I don't see the wherewithal, financially, to address it. It's a huge vacuum. I mean, I don't know how better to say it, and I don't know what we can do about it. I mean, Congress is going to have to come in and say, "Look, get some priorities here." $87 billion for Iraq is probably going to get adopted. But zero for ports? It's not a good balance.

Mr. GUERRERO. Senator Breaux, if I could put the needs in perspective, in our testimony, and also in our report, we have a table that shows, for selected grants, including grants for ports, the amounts that have been requested exceeded the amounts available by a factor of eight to one.

Senator BREAUX. Well, I——

Mr. GUERRERO. So the demand is very, very——

Senator BREAUX.—understand that. But if you have zero—I mean, there's nothing out there. I mean, the Coast Guard has estimated, as I understand it, that the ports would require $1.1 billion in security investments if we're talking about them implementing it—1.1 billion is what this gentleman says is going to be needed for the ports of this country to address their security needs, from a Federal standpoint. And we have requested—you have requested, the government has requested, zero.

So we can talk about how the requests greatly exceed the amount of money that is there, but when the Coast Guard says $1.1 billion is needed for security to the ports, and we request zero, there's a huge disconnect. There's a huge disconnect between what the Coast Guard is saying is needed for the maritime ports and what is being requested by others who make the request. Now, we can say that there is—if you let the ports make the request, you add it all up, it's going to be a gazillion dollars. But when the Coast Guard tell me it's 1.1, and the Administration says zero, that's the huge disconnect.

Mr. GUERRERO. Senator, I think I was trying to agree with the point you were making, that there is that huge disconnect, and I think the data shows that.

Senator BREAUX. Well, I mean, that—and I'm not beating on you guys, because you are the people we work with the closest. I mean, you understand the problem. But, I mean, there's only so much money, unless you don't worry about the deficit at all, which is $500 billion, and just keep adding to it. But for us to add another $87 billion for Afghanistan and Iraq for security, et cetera, and for rebuilding them, and to say we're going to allocate zero to the ports, when our own Coast Guard says it's a $1.1 billion requirement, there's something missing somewhere. There's a huge disconnect, in terms of priorities.

And I thank you for your diligence.

Senator LOTT. Senator Boxer?

STATEMENT OF HON. BARBARA BOXER,
U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Thank you so much, Mr. Chairman.

Mr. Chairman, this is not a happy hearing. I think the people sitting here are good public servants. But this is not a happy hearing, because, to say it directly, we are under-funding homeland defense. And you can sugarcoat it, and you can do everything you want, but that's the truth. And just as the President came to the microphone, finally, and said, "We need tens of billions of dollars for Iraq," someone has to come to the microphone and say what we need to keep our country safe, because September 11 changed everything, and this was the first attack of this nature in the continental United States.

Now, Senator Breaux did it today with port security. He basically said the emperor has no clothes. We're asking for all this money, more money to protect the ports in Iraq, than has been asked to protect us.

Now, I'm not going to ask you your questions on whether you agree or disagree with the budget. You're dealing with what the Administration has told you you've got. So I'm not going to put you in that situation. I mean, this is something that happens under Democratic and Republican administrations. The people who are fighting for their areas, you know, sometimes lose the fight around the table.

But we've got to be honest with the American people. We are vulnerable. Have we made some progress? Yes. Can we make more? Yes. Should we? Yes. And it is a question of priorities.

You know, when I go home, and I ask the people in my state, who have earned millions of dollars, if they need a tax cut or they would prefer it if their homeland was safe, let me tell you, to the person, they say, "Oh, you've got to be kidding. I've got enough. I've got enough plasma TVs to last a lifetime. I've got enough homes. I've got enough yachts. I've got enough airplanes." And, let me tell you, a lot of those people live in my state. Good, successful people. They don't want more money in their pocket. They want more money in your pocket. And port security is clearly necessary.

I just did a tour of the ports in California during this month, Mr. Chairman. It was really fascinating. All the way from the top of my state, Crescent City, down to Long Beach, in this particular tour. I've been to San Diego. I've been to every other port. And I have to say, it's all the same; they're worried. They're doing their best, but they're very worried.

And I want to show you what the FBI told us about the threat of shoulder-fired missiles. And they told us this in April—May 2002. Show it so that Senator Lott can see it. "Given al Qaeda's demonstrated objective to target the U.S. airline industry, its access to U.S. and Russian-made MANPAD systems, and recent apparent targeting of U.S.-led military forces in Saudi Arabia, law enforcement agencies in the U.S. should remain alert to the potential use of MANPADS against U.S. aircraft." That is a direct warning to us.

Now, since that time, there have been attempts to shoot down an Israeli commercial airliner and several of our military planes—most recently, the other day, a C–17 aircraft made in my state, an

incredible, incredible plane. Now, there but for the grace of God, those attempts were not successful.

Honest to God, I am begging you that you need to do all you can so we are not back in here after we have seen a plane brought down, or perhaps hit in some way, the airline industry on its back, and people saying, "You know what? It isn't worth it. I'll do a conference call. I'll drive to grandma's house."

It is unbelievable to me the pace at which we are moving. Now, we have companies telling us if they were able to move forward, they could begin installation within a few months. And I know, Admiral, that you care about this. And there is—I have spoken to Secretary Ridge, and he cares about this. But we are fooling ourselves. If we don't put the money behind it, nothing will happen. We saw what this great country could do.

We saw what we did in World War II with the "greatest generation." We saw this great generation of military men and women, what they did here, how we moved mountains to get them over there and how we won the military victory really quickly. Lots of other problems that we didn't plan for, as well.

But this is staring in our face, this FBI warning, and I am just so concerned that we are not treating this in the right way. I've been around here long enough—ten years in the House, ten years in the Senate. I served on the Military Committee in the House and also the Government Operations Committee, where we oversaw the FAA. I know bureaucratic talk from real talk, "We're examining, we're surveying, we're looking." This is an emergency circumstance.

$87 billion for Iraq and Afghanistan, a lot of that for rebuilding, a lot of that for protecting airports and ports. We're going to debate it, we're going to discuss it. The military will get what they need.

But I have to tell you, our people are vulnerable. And my message to you gentlemen, since—well, there is a woman here—ladies and gentlemen, is I don't—I want you to fight harder around the table. This is our country. Even if you have to take a little heat from some other folks over at OMB, who cares? Who cares? Their job is to cut budgets. Your job is to protect the country. And I'm worried, and I'm concerned. How we cannot sit here after the GAO report and say, "We aren't doing enough for our ports, Senators. And I'm going to take a risk, and I'm going to tell the President this, because if he really hears this from me, he will act." That's what I want to hear. I don't expect to hear.

But I hope you'll just take back my concern, as Admiral Loy said he would do that, because I don't have the questions. You're doing everything you can do within, you know, your parameters. Air marshals, arming the pilots, too slow. Too slow. You don't have enough air marshals. Let the pilots defend the aircraft, for God sakes. Only a couple of hundred? I agree with Senator Lott on that. This is something we can work together in a bipartisan way. Get the pilots trained. Most of them fought in the military. Don't tie their hands when you don't have enough air marshals. And all this moving Customs agents and all that. Frankly, I think that's just moving—it's like a shell game; it's not real.

Anyhow, you can tell my concern and my frustration, my fears. I want them to be allayed. I'm looking to you to do that, and I hope

that we can work together to make more progress than we're making.

Thank you.

Senator LOTT. Thank you, Senator Boxer.

And thank the panel for your time and testimony. We'll look forward to working with you in the future.

The Committee stands adjourned.

[Whereupon, at 11:25 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Thank you Mr. Chairman for calling this important hearing on transportation security. As you know, Thursday will mark the two-year anniversary of the horrible terrorist attacks of 2001. I see no better time to look into the progress of our national safety than today.

In 2002 we created the Department of Homeland Security by moving 22 agencies dispersed over 100 different government organizations. I believe the intention and consensus of this Committee was to consolidate those 22 agencies to provide a unified homeland security structure capable of responding to current and future threats. I will be interested to hear from the panel today whether that intention has/or will be accomplished anytime soon.

In my state of Montana we have a northern border with Canada that spans 630 miles which is equivalent to the distance from Chicago the Washington, D.C. and much of that border is rural. I will be interested to hear what progress has been made in northern border security. In the past, massive resources have been stationed along the U.S. southern border with Mexico and the northern border has been left vulnerable.

I look forward to testimony from Admiral Loy. Admiral Loy I commend you for the service you are paying your country but like many of my colleagues, I have been contacted by countless constituents regarding TSA over the last two years and much of the response has not been positive. For example, agriculture in my state is worried about the May interim final rule regarding hazmat background checks, which are scheduled to take effect in November. Rural businesses that provide petroleum and fertilizer are concerned these background checks will add another cost to their bottom line which is already troubled. I would like to hear the panels view on these broad rule making and I am curious to whether rural circumstances are considered before final rules are put out.

Finally, I am very concerned about the future of the Federal Flight Deck Officers Program. TSA seems to have a lack of enthusiasm for this program and its implementation. Myself, and many of my colleagues on this committee and in the entire body worked very hard to pass that program and to this point I have been less than enthusiastic about TSA's lackluster performance in implementing the program. I look forward to testimony on that program.

Mr. Chairman, again thank you for scheduling this important hearing and I look forward to the testimony.

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Over the last two years, the Congress has passed numerous bills and appropriated billions of dollars to protect our Nation's transportation system. Today we have the opportunity to review and assess the actions taken and discuss what additional tools and resources are needed to achieve our Nation's transportation security goals.

Being from an island state, air and ocean transportation are critical for the movement of people and goods where nearly 99 percent of all travelers arrive by air and 95 percent of all goods arrive by ship. Any disruption in these lifelines will jeopardize our island economy as well as threaten the health and well being of our residents and visitors.

Securing our Nation's immense, complex, and interwoven transportation system has been, and will continue to be, one of our greatest challenges. The United States has 5,525 miles of border with Canada and 1,989 miles of border with Mexico. Our maritime border includes 95,000 miles of shoreline, more than 360 maritime ports, and 3.4 million square miles of exclusive economic zone, 1.5 million square miles of which are in the Western Pacific.

In between our borders and coastlines are approximately 5,000 public use airports, including 430 commercial airports, 317 intermodal official ports of entry, 3.9

million miles of roads, 100,000 miles of rail, 2.2 million miles of pipelines, 500 train stations, and almost 600,000 bridges.

The challenges common to ensuring the safety of our Nation's diverse modes of transportation include:

- Coordinating numerous stakeholders, including federal, state and local governments and private businesses;
- Coordinating an intelligence system in order to effectively collect and analyze information;
- Developing and implementing the right technology to meet security needs;
- Adequately funding transportation security programs; and
- Ensuring safety of the transportation system without sacrificing efficiency.

I look forward to hearing from the distinguished witnesses on these important issues. I am most interested in hearing your thoughts on which programs are working, which are not working, and what additional resources you need to fulfill your missions.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED TO JEFFREY N. SHANE

Question 1. It is my understanding that prior to TSA's transfer to the Department of Homeland Security, DOT and TSA intended to sign a series of MOAs (Memoranda of Agreement) to clarify their roles and responsibilities. Why were the MOAs not signed and what is their current status? As you have read, MOAs are one of GAO's top recommendations.

Answer. TSA was created here at the Department of Transportation, and as such, we retain very close ties with TSA and its leadership. In fact, these relationships have helped us to develop close links throughout the new department, and we continue working closely with our former colleagues, supporting them every step of the way as they defend our Nation's homeland.

As noted in my written testimony, we have taken numerous actions to ensure that this close working relationship continues into the future as well. Just prior to TSA's transition to DHS, the Federal Aviation Administration and TSA signed a memorandum of agreement specifying the roles and responsibilities that each agency would play in overseeing the safety and security of our aviation system. Given the unique challenges we face in aviation security, the heavy emphasis in the Aviation and Transportation Security Act on specific deadlines for improving aviation security, and the FAA's continuing responsibilities for managing the air traffic control system, we believed that it was important to have a written agreement between DOT and DHS in this area.

Extensive, regularized lines of communication have been and are being established with emphasis on coordination. At present, we are working together effectively in areas where our responsibilities intersect. As our relationship continues to develop, and we gain additional experience, we intend to focus on identifying areas of common concern and determine the most effective means for formalizing our relationship. As a result of our communication and coordination over the past year—which includes a regular meeting with senior TSA staff on a bi-weekly basis to discuss current issues and ensure full cooperation between TSA and our modal administrations on security issues—we have begun to identify areas of DOT/DHS interaction that could benefit from formalization in written documents. When areas of recurring interaction between the two Departments have been sufficiently identified, we will work with DHS to pursue one or more additional memoranda of agreement to clarify the roles and responsibilities of the two Departments in those areas.

Question 2. What is DOT's role in transportation security?

Answer. Since the transfer of TSA to DHS, we have found that we continue to have a role in transportation security. Our statutory mission of providing for a safe, efficient and economically viable transportation system is inextricably linked to the security mission of DHS. The Department also provides a critical link to transportation stakeholders based on decades of experience working closely with those involved in various parts of the transportation system. This means that we must work hard to integrate smart and efficient security measures and ensure that they are developed with sufficient stakeholder input—to fail to do so can be dangerous or economically unsustainable. Additionally, in accordance with the Homeland Security Policy Directive, issued on December 17, 2003, the Department continues to collaborate with DHS on all matters relating to transportation security and transportation infrastructure protection.

To accomplish this, our Office of Intelligence and Security and Office of Emergency Transportation, in conjunction with each of the Operating Administrations, the Homeland Security Council and DHS components including TSA, FEMA and CBP and provides five primary services:

- *Policy:* Ensure transportation security policy complements safety, mobility and economic viability.
- *System Design:* Incorporate security policy decisions in the design of transportation systems and infrastructure (*i.e.,* bridges, tunnels, and transit systems).
- *Intelligence and Information:* Analyze and provide important security and economic intelligence to DOT customers, including DHS, offices negotiating international treaties, operating administrations, and to industry stakeholders, to the extent authorized by law.
- *Operations:*
  - —Monitor the real-time status of the transportation system. This historically proves valuable during emergencies, including the August blackout, Hurricanes (most recently Isabel), earthquakes and hazmat incidents.
  - —Provide emergency transportation services in support of the "all hazard" National Response Plan, which now expands our response and recovery functions to include terrorist attacks with our more traditional scope of accidents and natural disasters. This role, formerly under the Federal Response Plan, is one for which we are especially well suited and experienced.
- *Readiness:* In support of the new Homeland Security Presidential Directive on Preparedness, coordinate DOT's role in readiness and response exercises. We continue to be primary participants in exercises, including TOPOFF 2, Forward Challenge, Crimson Shield, Scarlet Cloud, and others. Virtually every safety or security-related exercise directly involves management of the transportation system.

Question 3. What share of DOT's work do you believe is security-related? Have the modal agencies shifted resources toward security-related initiatives since September 11, 2001?

Answer. In addition to the creation of TSA, each DOT modal administration aggressively pursued security initiatives in response to our post 9–11 realities. Since its creation on March 1, 2003, DHS has assumed primary responsibility for transportation security programs and initiatives. However, because of the complexity of the system and considerable expertise, DOT has played a direct supporting role in DHS's major transportation-related security initiatives. Resource expenditures by DOT on transportation security, including those cited below, are now coordinated with DHS and are consistent with DOT's ongoing responsibilities for the safety, mobility, and economic viability of the National Transportation System.

With that said, it is very difficult to quantify, in percentage terms, what share of DOT's work is security related. Some of the work cited below is directly related to DOT's ongoing role in transportation security, such as the Office of Intelligence and Security's continued support of national and homeland security policy development, and those critical infrastructure programs involving joint DOT/DHS legal responsibilities such as hazardous materials. The difficulty lies in quantifying the many efforts that benefit both security and safety or efficiency (dual use), or where we are attempting to build security into transportation rather than adding it as an expensive overlay, such as the Federal Transit Administration's regional security and response forums or Federal Motor Carrier Safety Administration's truck security prototypes.

The national strategies (National Strategy for Homeland Security and the National Strategy for the Protection of Critical Infrastructures and Key Assets) designated DHS as the lead for transportation critical infrastructure issues. DOT retains lead roles, however, in other critical areas:

- DOT and DHS share responsibility for hazardous materials transportation security per the Homeland Security Act of 2002. Much of the Research and Special Programs Administration's work revolves around the safe and secure movement of hazardous materials, including the Nation's pipeline infrastructure (800,000 surface shipments; 2.1 million miles of pipelines). The two agencies are working cooperatively on a number of fronts to address hazardous materials transportation security issues.
- DOT remains responsible for significant portions of our own internal (DOT owned and operated) infrastructure. This includes the physical and cyber security of the National Airspace System, consisting of about 1,000 staffed and

10,000 un-staffed facilities. The Infrastructure Protection Program for this system will cost $300 million. GPS augmentation sites critical to transportation applications, U.S. portions of the St. Lawrence Seaway, and vessels of the Ready Reserve Force are some other examples of critical DOT owned/managed infrastructure.

DOT Operating Administrations remain essential partners and contributors with DHS in nearly every transportation security program. A few examples of DOT contributions include:

- The Federal Aviation Administration operates the National Airspace System and, as the safety regulator of the aviation industry, works closely with DHS and TSA to ensure security of the airspace and industry through daily operations, policy and rulemaking.
- The Federal Railroad Administration currently employs about 457 inspectors that integrate safety and security in their track, operations and emergency plan inspections. In a joint effort with the Federal Transit Administration, TSA and DHS, FRA assisted both passenger and commuter rail systems with the development of System Security Plans. FRA inspectors assist DHS (U.S. Customs and Border Protection) with joint border crossing inspections using the Vehicle Cargo Inspection System.
- The Federal Highway Administration continues to work with DOD's Transportation Command to ensure adequate planning is conducted for strategic movement of military cargoes between military installations and port facilities.
- The Federal Motor Carrier Safety Administration is assisting TSA in implementing Section 1012 of the USA PATRIOT Act by developing security risk review procedures for all persons seeking issuance or renewal of hazardous materials endorsements of commercial driver's licenses.
- FTA and TSA have closely coordinated efforts to enhance transit system security. TSA is focusing on developing threat and vulnerability processes, standards for plans, and exploring advanced technologies. FTA is developing training forums to promote emergency preparedness and best practices, security design information, and facilitating chem-bio detection technologies for the unique transit environment.
- RSPA is working closely with TSA and pipeline operators to develop an understanding of pipeline security issues, share best practices, improve coordination among diverse stakeholders; plan for preparedness, response and recovery; and verify that significant major operators have acceptable security plans and programs. In consultation with DHS, they are conducting an assessment of hazardous materials transportation vulnerabilities and issued security regulations.
- The Maritime Administration provides strategic sealift capacity to support deployment of U.S. military forces for national security objectives through management of the Ready Reserve Force. During Operation Iraqi Freedom, MARAD coordinated the mobilization of 135 ships and over 5,000 crewmembers.
- DOT co-chairs with DHS the Asian Pacific Economic Cooperation Transportation Security Experts Group as well as Operation Safe Commerce, a program that funds the testing of industry solutions to the need for increased security in the international movement of intermodal containers.

Question 4. Last January I asked TSA and FRA to review Amtrak's security plan. Unfortunately, the plan on which you provided comments turned out not to be Amtrak's official plan. Have you had the opportunity to review Amtrak's official plan, submitted April 10, 2003 and do you have any recommendations for the Committee?

Answer. The Federal Railroad Administration directly provides the oversight and funding conduit for Amtrak's appropriated funds. The FRA routinely conducts validation reviews of Amtrak's financial activities and budget requests. The FRA reviewed both Amtrak's system security plan and the April 2003 security plan modifications for capital improvements. The FRA, in conjunction with TSA and Amtrak management and security officials, found the security plan satisfactory and the security-related capital improvements to be appropriate.

Question 5. What is the greatest security challenge facing your agencies and what actions are being taken to address the challenge?

Answer. The effective integration of security, as a cornerstone of transportation—alongside safety, mobility and economic viability—is our biggest challenge. America's ability to sustain smart security precautions and measures over the long term will depend entirely on how effectively and efficiently they are integrated into transportation system policy, design (*i.e.,* hardened bridges, multi-use databases, etc.)

and operations. Security, without appropriate consideration for costs and efficiency will not be effective. Only smart and efficient security measures that balance security with safety, mobility and sound economics will endure. In this way, our economy will grow and our people and goods move safely and securely.

DOT is actively pursuing this integration on several fronts. We have learned that, while much of transportation security resides in DHS; the integration of security into a system as complex as transportation requires a significant and ongoing coordination and cooperation between DHS and DOT. The Secretary of DOT has designated the Deputy Secretary as his primary liaison with DHS. The Deputy Secretary, with assistance from DOT's Office of Intelligence and Security, will work to maintain constant communication and information exchange with TSA. The Office of Intelligence and Security also leads a security working group, with participation from each DOT operating administration, along with TSA's participation, to address specific security issues. Within DOT, that office is also working with each operating administration to ensure that there is an adequate network to accommodate the expeditious flow of security related information throughout the Department.

I highlighted some of the specific actions we have taken, in cooperation with DHS, during my testimony before the Committee. For example, the Maritime Administration has worked closely with the Coast Guard and TSA to evaluate security at our Nation's ports. These evaluations enabled TSA to disseminate two rounds of port security grants, facilitating $262 million in security upgrades as a result. The Federal Transit Administration has shared its expertise by conducting $30 million in vulnerability assessments and security training of transit operators across the country. Additionally, the Research and Special Programs Administration has worked closely with TSA to ensure that the transportation of hazardous materials fulfills both safety and security requirements.

Finally, I personally have served as a co-chairman of the Executive Steering Committee that oversees the Operation Safe Commerce (OSC) program. Fifty-eight million dollars in OSC grants have been awarded by DHS to the three participating load center ports—Los Angeles/Long Beach, Seattle/Tacoma, and New York/New Jersey—and these grants will serve as an essential test bed for new technologies designed to provide greater security for freight containers as they move on intermodal journeys through global commerce.

Question 6. Do your agencies have sufficient authority to ensure transportation security? What action do you believe Congress needs to take to assist in your efforts to improve transportation security?

Answer. We believe that, in general, the Department possesses the authority it needs to carry out our statutory responsibilities. Where we see the need for additional authority or for clarification of existing authority we will develop appropriate legislation on behalf of the Administration, as in the Administration's railroad safety reauthorization proposal, which was submitted to Congress in July 2003. Recognizing that, in some situations safety and security issues are woven together, we value the emphasis that Congress, in sections 1710 and 1711 of the Homeland Security Act, placed on the joint nature of DOT's security responsibilities with DHS for rail transportation of all cargoes, and for hazardous material transportation by all modes. This statutory authority gives us a clear basis on which to work even more closely with DHS on these two areas. Of course, the Federal Railroad Administration coordinates closely with the Department of Homeland Security wherever its exercise of safety authority would have security implications.

There are two areas in which we need the continued support of Congress in order to succeed in our mission.

- We seek your continued support for the resources necessary to sustain our links and important services to DHS and TSA. This comes in three key areas:

  (1) It is critical for DOT to have the appropriate resources—staff and budget—to assist in the development of transportation-related security policy, system design, intelligence and information and readiness. This will enable DOT to be an effective partner with DHS as both Departments deal with the integration of transportation security measures into the transportation system while maintaining safety, mobility and economic viability.

  (2) DOT must maintain the emergency transportation capabilities for response to all hazards, ranging from terrorist attacks to natural disasters like hurricanes and earthquakes. This unique capability has been developed and honed within DOT and demonstrated effectively, most recently during Hurricane Isabel.

  (3) We need to have appropriate resources to plan and participate in readiness exercises like Topoff 2, Determined Promise, Forward Challenge, and oth-

ers. Although the new Homeland Security Presidential Directive on Preparedness will improve coordination and effectiveness of exercises and other pre-incident activities, it will require increased DOT involvement to succeed.

Within DOT, the three functions discussed above are primarily accomplished through the Office of Intelligence and Security, and the Research and Special Program Administration's Office of Emergency Transportation. Together these small staffs provide valuable support in security policy, system design, intelligence, emergency preparedness, readiness and response operations.

If need arises, we will seek your support in legislation that clarifies DOT's role in security policy decision making, and in the emergency transportation services provided to DHS.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED TO ADMIRAL THOMAS H. COLLINS

MTSA Compliance Costs and Port Security Grants

Question 1. I understand the Coast Guard estimates the private sector costs for compliance with the requirements of the Maritime Transportation Security At to be $4.4 billion, with annual costs of $500 million. Since the September 11 attacks, Congress has provided a total of $348 million for port security grants. While the Administration's Fiscal Year 2004 budget requests $38 million for the

Department's Directorate of border and Transportation Security for grants, subsidies, and contributions and $51 million for the Department's Directorate of information Analysis and Infrastructure Protection for the same purpose, it is unclear what these requests are for. Additionally, it is unclear whether or not these line items will fund the maritime and port security grants to be awarded in accordance with the Maritime Transportation Security Act. Is this $4.4 billion figure accurate? If so, what is it based on? How much is the Administration requesting for maritime and port security grants for Fiscal Year 2004? Which agencies or directorates will be managing these funds? While I understand the Coast Guard will not directly administer these funds, what role does the Coast Guard play in awarding these grants? Can you explain how the awarding of these grants will be coordinated with Port Security Assessments being identified by the Coast Guard as part of your ongoing assessments? In light of this $4.4 billion backlog, do you think the Administration's request is adequate to address these vulnerabilities?

Answer. The $4.4 billion figure contained within this question is not accurate. As part of the rulemaking process, the Coast Guard conducted an assessment of the cost to industry of implementing the SOLAS Amendments, the ISPS Code and Section 102 of the MTSA. The final rules published October 22, 2003 estimates the MTSA implementation costs to industry to be $1.5 billion. Following implementation, the annual cost is approximately $884 million for a total of $7.331 billion over the next 10 years.

In the DHS FY 04 budget, $125 million was appropriated for port security grants. The Transportation Security Administration (TSA) manages the grant funds and administers the grant process in cooperation with the Maritime Administration (MARAD) and the Coast Guard. Coast Guard Captains of the Port and MARAD Region Directors provide the first level of review and prioritization within the grant requests. A National Level Selection Board consisting of the Undersecretary of TSA, the Commandant of the Coast Guard, and the Administrator of MARAD, or their representatives, constitutes the final grant approval body.

A prerequisite for submitting physical and operational security enhancement proposals is the completion of a security assessment, the findings of which are incorporated into determining the grant selection criteria in partnership with TSA and MARAD. The required assessment does not have to be a Coast Guard Port Security Assessment, but the Coast Guard does make PSA findings available to applicants and port security committees for use in developing grant proposals. However, a port that has not received a PSA is not be penalized during the grant evaluation process.

While clearly there is a governmental role in providing port security, vessel and facility owners and operators have a shared responsibility to provide port security measures. The requirements contained on the final rule are intentionally performance based to allow innovative and cost-effective solutions by industry to improve security with minimum capital outlay and burden on legitimate use of the maritime transportation system. In light of this and the numerous additional initiatives that have been undertaken by the Federal Government to improve maritime security, the Coast Guard believes the Administration's request is adequate.

MTSA Facility Security Rules

Question 2. On July 1 of this year, the Coast Guard proposed seven rules implementing requirements of the Maritime Security Act. Doing all seven at once is ambitious, but I want to commend you and your staff for pushing forward with this very important work. One of the proposed rules would establish requirements for facility security. I understand several of the requirements have caused some concern within the maritime industry. Specifically, facility owner and operators would be required to establish "waterborne security patrols" for "examination of piers, wharves, and similar structures . . . for the presence of dangerous substances and devices underwater." While I agree this is an important part of facility security, it is my belief that security in U.S. waters is inherently a government function that must be performed by a law enforcement officer. Can you explain the Coast Guard's view on this issue?

Another Proposal within the rule regarding facility security would require the facility to have the capability to "be able to check cargo entering the facility for dangerous substances and devices at the rate specified in the approved Facility Security plan (FSP). I may be a bit confused, but I was under the belief that the Bureau of Customs and Border Protection was responsible for screening inbound and outbound cargo and had in fact received considerable increases in appropriations to increase these capabilities. Is this correct, and if so, why are we requiring this of facility operators?

Answer. On July 1 of this year, the Coast Guard published six temporary interim rules to promulgate maritime security requirements mandated by the Maritime Transportation Security Act of 2002. The Coast Guard believes owners and operators have the authority to implement the identified security measures. The final regulations published on October 22, 2003 do not require owners or operators to undertake law enforcement action, but rather to implement security measures consistent with their longstanding responsibility to ensure the security of their vessels and facilities as specifically prescribed by 33 CFR 6.16–3 and 33 CFR 6.19–1. It is also important to note that the security measures identified only relate to MARSEC Level 3 implementation and do not include Coast Guard and/or other Federal Government maritime security efforts.

We recognize that screening for dangerous substances and devices is a complex and technically difficult task to implement. In the final rules published on October 22, 2003, we have clarified that cargo checks should be focused on the cargo arriving at or on the facility or vessel to detect evidence of tampering or to prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or operator.

Sharing the Infrastructure Burden of AIS

Question 3. GAO has pointed out that implementation of the Automatic Identification System (AIS) could require substantial Federal infrastructure investment in new Vessel Traffic Service systems for U.S. cities to receive and process important security information transmitted from vessels. Installation and training costs for this infrastructure could cost more than $100 million. To reduce the budgetary burden on the Federal Government, has the Coast Guard and DHS considered partnering with local entities to provide the VTS service and share in its costs-such as in the case at the Los Angeles/Long Beach VTS?

Answer. The Coast Guard has completed many Ports and Waterways Safety Assessments to specifically determine the need for VTS systems in other ports. A VTS system is not needed in every port to use the AIS information for security purposes.

In non-VTS ports, implementation of AIS receive/transmit capability will be accomplished through cooperative arrangements with Federal, State and local stakeholders on integrated command center projects such as the Joint Harbor Operations Centers in Hampton Roads, Virginia and San Diego, CA, as well as through the Rescue 21 and the Integrated Deepwater System projects. The Coast Guard is continuing to partner with local entities and is also leveraging efforts already underway in other areas. For example, the Coast Guard is receiving AIS information from the St. Lawrence Seaway Development Corp, the Department of Justice SEAHAWK Project in Charleston, SC, and the Joint Maritime Operations Center (JMOC) in Seattle, WA. The DOJ SEAHAWK project is an inter-agency effort to establish a port security command center and will include AIS capability integrated with other sensor information. A similar approach is being pursued for the JMOC.

Review of Pilot Port Security Assessment Reports

Question 4. Given the importance of and expense involved with the Port Security Assessments (PSA), do you plan to enter into another contract with Northrop for additional PSAs before a thorough evaluation of the pilot assessments are completed

and a new methodology is devised? How long will the Coast Guard's evaluation of the pilot projects take and do you plan to get any independent viewpoints (outside of DHS) on the process before finalizing it and awarding additional contracts for these PSAs?

Answer. No additional work will be contracted with Northrop Grumman Mission Systems until we have evaluated the pilot port reports (Huntington & Tampa) and determined that the quality of their work warrants awarding of future work in support of the PSA program.

The Coast Guard decided to test the revised PSA assessment methodology (version 2) on the ports of Tampa, FL and Huntington, WV to ensure that the report added value to the Captains Of The Port (COTP) and their Area Maritime Security Committee in drafting Area Maritime Security Plans. The draft pilot reports were delivered to the Coast Guard on 20 October 2003, and the final reports were delivered on 19 November. During our review of the draft reports for these two pilot ports, we identified areas that need further modification. These modifications are a result of the lessons learned though the pilot process, changes in the maritime security environment as a result of the publication of the MTSA of 2002 Final Rules, and the development of industry self-assessment methodologies. DHS has also provided guidance that impacts what areas/facilities we are to focus on during our PSAs, and many stakeholders have completed their own assessments. In order to accommodate these changes and provide a more dynamic report, the PSA program is moving onto a PSA version 3 (V3).

The draft pilot reports have been supplied to the respective Coast Guard COTPs, as well as the pertinent port stakeholders in each pilot port, for comment. To the extent that they are applicable, comments from these primary users of the PSA report will be incorporated into the development of the V3 assessment methodology. Additionally, before the Coast Guard fields teams to conduct V3 PSA, the PSA staff will present the intended approach to a sampling of COTPs and Coast Guard Area/District staffs. Comments and observations from the GAO will also be incorporated into this revised methodology, which should be fielded with the support of multiple contractors sometime in early 2004.

PSA Program Duplication of Assessments

Question 5. What is the Coast Guard doing to avoid duplication of security assessments done by port stakeholders?

Answer. The Coast Guard Port Security Assessment program has changed to reflect the availability of vulnerability assessments by marine facilities and other entities. The new focus of the program is providing the Federal Maritime Security Coordinator and Area Maritime Security Committee with a terrorist evaluation of the waterway and navigation system in the ports. The program is also providing a database tool that integrates the available assessments and response capabilities from all sources and displays the information in a layered, geospatial format to assist in security planning. This evolution of the program avoids duplication of effort and provides additional critical information for each port to improve their countermeasure development and incident response capabilities.

Lead Agency on Maritime Security

Question 6. Which agency within DHS is the lead agency on maritime security? Which agency do you believe is best equipped to take the lead role in maritime security?

Answer. The Coast Guard is the lead Federal agency for maritime security. However, the Coast Guard will continue to work closely with its DHS partners from the Information Analysis, and Infrastructure Protection (IADP) Directorate and the Boarder and Transportation Security (BTS) Directorate (which includes the Transportation Security Administration (TSA) and the Bureau of Customs and Border Protection (CBP)) which each have important roles to play in maritime security.

Lead Agency on Cargo Security

Question 7. Which agency within DHS is the lead agency on cargo security? Which agency do you believe is best equipped to take the lead role in cargo security?

Answer. The Border and Transportation Security Directorate's (BTS') Customs and Border Protection (CBP) is the lead agency on cargo security.

As the single unified border agency of the United States, CBP is best equipped to protect America and the American people as lead agency for cargo security in order to facilitate the flow of legitimate trade and travel.

International Efforts to Improve Transportation Security

Question 8. What efforts are underway internationally to improve transportation security?

Answer. The answer provided below focuses on international "maritime" security.

The Coast Guard actively participates in several international forums such as the International Maritime Organization (IMO), International Labor Organization (ILO), the G–8, and the Asia Pacific Economic Cooperation (APEC) to develop international security standards and encourage harmonization of maritime security.

Based on IMO guidelines, the Coast Guard conducts security audits of foreign port passenger terminals as required by the Omnibus Diplomatic Security and Antiterrorism Act of 1986. Audit findings are provided to Department of State and to the host government via the local American Embassy/Consulate.

To assess the effectiveness of antiterrorism measures maintained in foreign ports as required by the MTSA, the Coast Guard is developing a Foreign Port Security Audit Program. This effort began in FY 2003 with a foreign port assessment team in the Latin American/Caribbean region that was organized and funded by DOD. Southern Command (SOUTHCOM) and led by MARAD and included the Coast Guard and Customs and Boarder Protection (BCBP) personnel. MARAD was assigned the responsibility of field assessment team chief, development of a comprehensive cargo security assessment tool, field methodology, and production of Assessment Team reports to SOUTHCOM for subsequent use by the involved U.S. embassies. Beginning in FY 2005 the Coast Guard will assume the lead for these assessments as mandated by the Maritime Transportation Security Act (MTSA) of 2002, Section 109. Using the International Maritime Organization International Ship and Port Facility Security (ISPS) Code and the ILO Code of Practices for Port Security (currently under development to assist countries in the development of port security plans) as a baseline, the Coast Guard will audit foreign countries' compliance with these international standards. The Coast Guard will work with other elements of the Department of Homeland Security as well as other agencies (DOS, DOD, MARAD, and Treasury) to prioritize countries and to carry out the audits. The audit will include physical visits to a sample of ports in each country to verify country compliance. This process will start after the implementation date of the ISPS Code on July 1, 2004 and result in the audits of approximately 30–40 countries annually. If the audit findings indicate that adequate antiterrorism measures are not maintained, the MTSA requires the Coast Guard to notify the country and in conjunction with Department of State develop a port security training program for foreign officials as may be required. During FY 2003, two courses were conducted under the Inter-American Port Security Training Program (IAPSTP), which is funded by the Organization of American States (OAS) and organized, managed, and executed by the U.S. Maritime Administration (MARAD) for the OAS. The IAPSTP was developed in cooperation with the OAS Inter-American Committee on Ports to provide port security training courses for port authority police and security personnel from OAS member countries of Central and South America, and the Caribbean. By November 2003, a total of 550 personnel had received IAPSTP training since its commencement in 1998. The four courses conducted each year account for 200 personnel trained. MARAD and OAS funds to conduct assitional courses in 2004.

Each year the Coast Guard provides assistance to approximately 60 countries worldwide. This assistance has been in the form of sales of new and excess materiel (*e.g.,* ships, patrol boats, etc.), resident training, exportable training, and temporary maritime advisors to host nation navies or coast guards. Through provision of Coast Guard expertise in ship handling, maritime law enforcement, boarding officer and team member training, port security vulnerability assessment and professional development for maritime officer and enlisted corps, host nation navies and coast guards become force multipliers in the global war on terrorism.

International Aviation Security Initiatives

The Department of Homeland Security actively promotes the strengthening of international standards and recommended practices for aviation security through the International Civil Aviation Organization (ICAO) and G–8 consultations, as well as within the framework of a formal and continuing dialogue with the European Union, the European Civil Aviation Conference, Asia Pacific Economic Cooperation, and other regional entities.

In October 2001, a meeting of the International Civil Aviation Organization (ICAO) Aviation Security Panel was held to consider changes in international aviation security standards in light of 9/11. The Aviation Security Panel holds responsibility for promulgating international security standards and includes as a member the U.S. Government represented by TSA's Director of International Affairs. TSA proposed, and the Panel accepted, changes to amendment 10 of Annex 17 (the document that sets forth international aviation security standards) that elevates several

recommendations to the level of standards and provides language for the new standards.

Ministers and other high-level officials from 154 countries and 24 international organizations met in February 2002 to endorse the creation of a mandatory aviation security audit program, drawing upon the expertise of the Aviation Security Panel, the TSA's Foreign Airport Assessment Program, and other existing, viable programs. The mandatory audits are intended to determine a State's compliance with international standards by observing measures at airports and assessing the State's capabilities to sustain those measures.

As a demonstration of U.S. support, the TSA committed and provided U.S. $1 million as an initial injection of funds to the Aviation Security Mechanism specifically for the development of the security audit program. ICAO now has a roster of certified auditors totaling 70 aviation security experts, representing 39 States from across all ICAO regions. 20 audits are expected to be completed by the end of 2003, and 40 audits each year thereafter. ICAO's goals are to complete a total of 60 audits by the end of 2004 and to audit all 188 ICAO contracting States within five years.

TSA also influences the work of ICAO and the setting of international standards by developing and supporting initiatives within the framework of the Group of Eight (Canada, Germany, France, Japan, Italy, U.S., Russia, and U.K.). The most recent initiative, which was agreed upon at the G–8 Summit in June 2003, called for the continued support for the implementation of the ICAO Security Audit Program by all ICAO Member States. Agreement was also reached to implement national measures to combat the threat to civil aviation from the illegal use of surface-to-air missile systems by terrorists, to reduce their proliferation and strengthen control of stockpiles by G–8 and other states and to promote the application of Wassenaar Arrangement principles to MANPADS export controls. Most of the work on MANPAD within the G–8 has been focused on proliferation; the area of developing and implementing appropriate countermeasures has not been addressed. In light of this, the U.S. has recommended to the G–8 in a recent meeting of the Roma/Lyon group that G–8 countries establish a working group to develop and agree upon a methodology to be used by G–8 countries in assessing an airport's vulnerability to the threat of MANPADS.

RESPONSE TO WRITTEN QUESTION SUBMITTED TO PETER GUERRERO

Question. Given GAO's extensive body of work on security issues, what do you believe are the top three challenges the Nation faces in securing the Nation's transportation system?

Answer. Transportation stakeholders face numerous challenges in securing the Nation's transportation system. Three significant challenges include: determining the appropriate level of security for all modes of transportation; coordinating among the various stakeholders and funding security improvements. First, the size of the transportation system makes it difficult to adequately secure. For example, the transportation system includes about 3.9 million miles of roads, over 100,000 miles of rail, almost 600,000 bridges, over 300 ports, 2.2 million miles of pipeline, 500 train stations, and over 5,000 public-use airports. The size of the system simultaneously provides a substantial number of potential targets for terrorists and makes it difficult to secure. Second, the number of stakeholders—including over 20 Federal entities, state and local governments, and hundreds of thousands of private businesses—can lead to coordination, communication, and consensus-building challenges. For example, representatives from several state and local government and industry associations told us that their members are receiving different messages from the various Federal agencies involved in transportation security. Finally, funding security improvements to our transportation system is challenging. The sluggish economy has weakened the transportation industry's financial condition by decreasing ridership and revenues. While the Federal Government has provided additional funding for transportation security since September 11, demand has far outstripped the additional amounts made available. A risk-based approach will be needed to target available funds to the most pressing needs.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. ERNEST F. HOLLINGS TO ADMIRAL JAMES M. LOY

Question. I understand that on July 28, 2003, you denied a petition submitted by Midway Airlines on May 31, 2002 for an adjustment to the Aviation Security Infrastructure Fee due in accordance with the *Aviation Transportation Security Act.*

When Congress approved the ATSA, we included language requiring airlines to pay to TSA a fee to cover its cost of providing increased civil aviation security services. We capped the amount you could collect as the amount the carrier paid for airline security in 2000.

During the hearing, we talked about the funding crises you are facing at TSA. I did not originally support the remittance of the fee for many reasons, but ultimately agreed to the remittance.

Apparently, with the denial by TSA of the petition, Midway will be required to pay TSA for the time period. Congress gave all carriers a "fee holiday" as part of the Emergency Wartime Supplemental Appropriations Act on April 16, 2003, that provided reimbursement to airlines for security costs that they paid to TSA. Had Midway paid the full amount due, it would have been fully reimbursed for these fees. However, because it paid only a percentage of the fee TSA claims it owes, it received only a percentage in return, leaving the balance outstanding. Now, after passage of this reimbursement provision, TSA demands that Midway pay the remaining balance.

If Midway does repay the remaining balance, would Midway be entitled to receive reimbursement for that amount under the Appropriations Act? If so, does TSA have monies left under the Appropriations Act to repay Midway?

If no monies are available to repay Midway, wouldn't that result in Midway being the only airline in the Nation that must pay the security infrastructure fee without reimbursement.

Please provide an explanation for what appears to be a unique situation.

Answer. The Emergency Wartime Supplemental Appropriations Act of 2003, (P.L. 108–11) provided TSA $2.3 billion to compensate U.S. air carriers for their expenses and any revenue forgone that related to aviation security. Rather than providing a reimbursement of TSA security fees, Congress provided this additional funding and specifically stated in the Act that U.S. air carriers would be compensated based on the ratio of security fees paid to TSA by each U.S. carrier compared to the total fees paid to TSA by all U.S. air carriers.

The statutory language of the Act stipulated only the security fees remitted to TSA by the date of enactment, April 16, 2003, were to be considered in determining distribution of the relief funds. Therefore, the amount of unremitted fees could not be taken into account in calculating the relief. Based on the statutory formula and the amount remitted by Midway Airlines to TSA by April 16, 2003, TSA issued a payment to the carrier of nearly $1.4 million.

The Act also required TSA to distribute the funding within 30 days of the enactment of the Act. Accordingly, TSA obligated or disbursed the funding within that time-frame based on the required formula and, therefore, does not have any relief funds remaining. As noted above, since Midway did not fully pay the fees by April 16, 2003, as specifically required by the Act, it is not entitled to additional compensation.

Although the Act suspended collection of the fees for 4 months as discussed below, it did not provide for cancellation of debts from unremitted security fees due before the suspension. TSA does not have the authority under the Debt Collection Improvement Act of 1996 to waive this indebtedness under these circumstances. Thus, the fees owed by Midway Airlines are still owed to the United States.

Midway Airlines is not unique in not receiving relief from its un-remitted security fee debt. TSA is collecting past-due fees from other carriers, which like Midway, had failed to follow the law and regulations and timely pay their fees. Based on the specific language of the Act, and as described above, TSA has denied all such requests for relief.

The Act did provide a separate relief measure to domestic and foreign air carriers by suspending both the passenger and air carrier security fees ("fee holiday") for all air carriers from June 1, 2003, through September 30, 2003. In addition to the nearly $1.4 million in direct relief, this separate measure provided Midway Airlines additional relief of approximately $612,000 in suspended fees.

Finally, TSA responded to concerns about assessing the security fee at the carrier's year 2000 screening costs since a number of the carriers, including Midway Airlines, now operate at a significantly reduced level compared to year 2000. Although the Aviation and Transportation Security Act (ATSA) authorizes TSA to charge the security fee up to each air carriers' year 2000 screening costs, it also grants TSA the authority to adjust the fee based on market share beginning in Fiscal Year 2005. TSA is working to ensure that a new air carrier fee structure, based on market share or another appropriate measure, is implemented as close as possible to October 1, 2004. TSA has already issued a notice in the *Federal Register* (68 FR 62613) requesting industry proposals on the methodology to be used in assessing future security fees.

WRITTEN QUESTIONS SUBMITTED BY HON. RON WYDEN TO
ADMIRAL JAMES M. LOY

On August 1, 2003, the Transportation Security Administration's (TSA) published a Federal Register Notice (68 Fed. Reg. 45265) concerning its plans to develop and implement a new version of the Computer Assisted Passenger Prescreening System, commonly known as "CAPPS II." I believe that this Notice was a positive first step in explaining to the public TSA's plans for CAPPS II, and in providing information needed to assess the program's potential impact on privacy. However, the Notice also left me with a number of questions as to how CAPPS II would operate. I believe that the answers to these questions are crucial to understanding the nature and implications of the system TSA is proposing. My questions fall into six main areas.

Question 1. What goes on in the "Risk Assessment" Portion of the Process

According to the explanation contained in the August 1 Federal Register Notice, CAPPS II will involve two main steps. The first step is authentication, in which the system will compare PNR data with data contained in commercial databases "for the sole purpose of authenticating passenger identity." The result will be a numeric score showing the confidence level that the identity the passenger provided is accurate.

The second step is the risk assessment. This is an area where I believe the explanations to date have been insufficient, making clarification essential.

Question 1a. The Federal Register Notice states that "[t]he risk assessment function is conducted internally within the U.S. government." Does this mean that, for purposes of the risk assessment, CAPPS II will not in any way query or otherwise make use of commercial databases?

Question lb. If the risk assessment process does not involve making additional queries of commercial databases, then what information *does* it rely on? At a minimum, it appears that the risk assessment will involve checking to see if the passenger is on any Federal list of known or suspected terrorists, or persons with outstanding arrest warrants for violent crimes. But are there additional sources of information, inside or outside government, that the risk assessment will use? Or does the risk assessment simply produce a "yes or no" answer as to whether the passenger is already on a government list of persons considered dangerous?

Question 1c. Checking against existing government watch lists seems like a straightforward way of determining whether a passenger is already known as a terrorist or suspected terrorist. But according to the Federal Register Notice, the risk assessment process will do more than that it will determine the likelihood that the passenger has "identifiable links" to known terrorists or terrorist organizations. How can the risk assessment process ferret out such links, if the information it relies on consists of existing government watch lists? Is it envisioned that the government will compile lists of all persons who have *any link* with a known terrorist or terrorist organization? Wouldn't this be an exceedingly broad list?

Question 1d. For example, suppose that a passenger once shared an apartment or college dorm room with a person who is now on a U.S. list of known terrorists. Would the risk assessment capture this link? If so, how? Would the risk assessment process check commercial databases, which may contain records of the passenger's past addresses? Or is it envisioned that this passenger would already be on a government watch list, based on this solely on this possibly innocent link?

Question 1e. The Federal Register Notice says that CAPPS II will generate a "risk score" for each traveling passenger. Is this "risk score" the product solely of the risk assessment process, or does it does it take into account the results of the authentication step as well? If the latter, does it factor in any data or information from the authentication process other than the numeric authentication score?

Question 1f. Suppose a passenger is *not* on a government watch list of known or suspected terrorists. Could the CAPPS II system nonetheless produce a high enough "risk score" to bar the passenger from flying?

Question 2. Process for Detecting and Correcting Mistakes

The Federal Register Notice states that a passenger will be able to request access to the PNR data CAPPS II contains on him/her, and to request the modification of that data if the passenger believes it is inaccurate. However, the Notice goes on to observe that because CAPPS II will not retain data on passengers for any significant time, in most cases there will be nothing for the passenger to obtain or correct.

Question 2a. This suggests that, while a procedure for accessing and requesting modifications to records may be important in other contexts, this approach really isn't very useful for addressing mistakes that may occur under CAPPS II. Does TSA agree that CAPPS II is going to require other types of redress procedures?

Question 2b. For example, if the system repeatedly flags a particular individual as suspicious, what options will that individual have to rectify the problem? Suppose the problem stems from inaccurate information in a commercial database, which results in a low authentication score for that individual. In such a case, accessing records held by the CAPPS II system would be useless. How will the system deal with mistakes of this kind?

Question 2c. What is the justification for exempting CAPPS II from the Privacy Act's data access and correction requirements?

Question 3. Accuracy of the "Identity Authentication" Part of the Process

The Federal Register Notice states that "[o]ne of TSA's primary purposes in creating this new system is to avoid the kind of miscommunication and improper identification that has, on occasion, occurred under the systems currently in use. During the test period, TSA hopes to confirm that the use of the CAPPS II program will significantly reduce improper identification."

However, a recent *Associated Press* article ("Feds Don't Track Airline Watchlist Mishaps," by David Kravets, July 23, 2003) reported that TSA does not keep information on the number of people who are misidentified and wrongly delayed or barred from flights under the current system.

Question 3a. Does TSA have any systematic way of tracking how often the current system makes mistakes?

Question 3b. If not, how will TSA determine whether and to what extent CAPPS II will reduce the number of cases of mistaken identity?

Question 3c. To what extent will TSA make public the results of its testing on the accuracy of the identity authentication process? Will the public be permitted to see the numbers behind any claimed decrease in misidentification—and to evaluate the rate at which mistakes still occur under the new system?

Question 4. Financial and Health Data

The Federal Register Notice states that the CAPPS II system "will not use measures of creditworthiness, such as FICO scores, and individual health records." However, this statement appears in the explanatory "Supplementary Information" section of the Notice. In what appears to be the official portion of the Notice the part headed "DHS/TSA 010"—there is no reference to such a limitation.

Question 4a. What is the *legal effect* of the statement in the "Supplementary Information" section that CAPPS II will not use individual financial and health information?

Question 4b. Why is there no comparable statement in the body of the official Privacy Notice itself?

Question 4c. The Notice makes the CAPPS II system "exempt from publishing the categories of sources of records." Why is TSA claiming this exemption? As a legal matter, wouldn't this permit TSA, a year or two down the road, to reverse its decision to refrain from using individual financial and medical data—and to start using such data without telling the public? How can the public rely on any current TSA description of what information the CAPPS II system will or will not use, if TSA is reserving the right to expand or modify the information it uses without any public notice or scrutiny?

Question 5. Procedures for Future Changes to CAPPS II

As noted above, the Notice makes CAPPS II "exempt from publishing the categories of sources of records." It also gives the CAPPS II system a security classification of "classified, sensitive."

Given this classified status and the exemptions from the Privacy Act, could TSA modify significant aspects of the CAPPS II program without disclosing the changes to the public? To what extent would TSA have the ability, from a legal perspective, to depart from the CAPPS II system description set forth in the Notice? Could a future TSA elect to make changes regarding the scope or operational characteristics of the CAPPS II system—and do so secretly, without a formal and public regulatory process? How easily could the various representations and assurances made in the Notice be withdrawn?

Question 6. Intended Future Link to Immigration Data

The Federal Register Notice states that "[i]t is . . . anticipated that CAPPS II will be linked with the U.S. Visitor and Immigrant Status Indicator Technology (US–VISIT) program at such time as both programs become fully operational, in order that processes at both border and airport points of entry and exit are consistent."

Question 6a. If the sole mission of the CAPPS II system is to determine whether a passenger may pose a risk to aviation security, why does the system need to be

linked with immigration data? Is it anticipated that CAPPS II may eventually be used not only for safeguarding aviation security, but also for enforcing immigration law for example, for apprehending illegal aliens or visitors who have overstayed their visas?

Question 6b. What are the specific "processes at both border and airport points of entry and exit" to which the Notice refers? What are the specific types of potential inconsistencies that TSA hopes to avoid by linking the CAPPS II and US–VISIT systems? Please provide some concrete examples of problems that could arise if the two systems were not linked.

WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO ADMIRAL JAMES M. LOY, HON. ROBERT C. BONNER, PETER GUERRERO, JEFFREY N. SHANE AND ADMIRAL THOMAS H. COLLINS

Question for Admiral Loy and Commissioner Bonner. The Department of Homeland Security (DHS) has proposed cutting the port security grant program by $105 million. Does the Administration still propose this cut?

Question for Admiral Loy and Mr. Guerrero. I am concerned that DHS and the Transportation Security Administration (TSA) are dealing with our nation's pressing life and death security needs by playing shell games with critical resources. Last week, Secretary Ridge announced that 5,000 new air marshals would be trained, but that these individuals would come from the existing ranks of custom and immigrations agents. During high-threat periods, this cross-training plan might enhance air security but will come at the expense of border and ground security. Under the Administration's plan to utilize current immigrations and customs employees to double as air marshals, how will DHS ensure that, during high-threat periods, there are adequate personnel to function both in air marshal roles and at the border as customs/immigrations agents?

Are any new air marshals currently being trained?

Question for Admiral Loy and Mr. Guerrero. Similarly, DHS has recently tried to divert $30 million from the Operation Safe Commerce pilot program intended to identify and implement the systemic port security initiation in order to cover a budget shortfall in airport security. Do you believe Federal port security programs are adequately funded?

Question For Undersecretary Shane. Recently, the Columbia Accident Investigation Board (CAIB) reported its findings on the shuttle accident on February 1. That Board found an intricate link between the poor safety culture, poor communication structure, and high level of outsourcing, or use of contractors, in the program. If the Administration truly believes that the safety and security of the American people is a top priority, why does it continue to press for outsourcing of our air traffic control system? Other countries have tried privatizing their air traffic control systems, and the results have been disastrous. What lessons do you feel we can learn from this CAIB report and from other countries with respect to the U.S. air traffic control system?

Question for Admiral Collins. The Maritime Transportation Security Act of2002 requires DHS to conduct vulnerability assessments of the nation's 55 largest seaports. At the current rate that they are being conducted, these assessments will not be completed for another *five* years. What is being done to expedite the completion of these vulnerability assessments?

Question For Admiral Collins, Admiral Loy, And Commissioner Bonner. The President has said that the transfer of weapons of mass destruction into the hands of terrorists is the gravest danger facing U.S. and global security. Please update me on DHS's efforts to improve the security of our ports by deploying detectors that can identify dangerous radioactive material hidden in containers on vessels. Also, please update me on DHS efforts to designate secure shipping lanes that meet an objective standard of security for origin-to-destination shipping.

Question for Admiral Loy. When does TSA plan to issue standards for security training of cabin flight crew members?

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO GERALD L. DILLINGHAM AND MARGARET WRIGHTSON

Question 1. I am concerned that DHS and the Transportation Security Administration (TSA) are dealing with our Nation's pressing life and death security needs

by playing shell games with critical resources. Last week, Secretary Ridge announced that 5,000 new air marshals would be trained, but that these individuals would come from the existing ranks of custom and immigration agents. During high-threat periods, this cross-training plan might enhance air security but will come at the expense of border and ground security. Under the Administration's plan to utilize current immigration and customs employees to double as air marshals, how will DHS ensure that, during high-threat periods, there are adequate personnel both in air marshal roles *and* at the border as customs/immigration agents?

Mr. Dillingham's Answer. DHS's plan does not explicitly address the adequacy of the current immigration, customs, and air marshal workforces to address concurrent high threats to border, ground, and aviation security. Rather, the plan provides for temporarily enhancing the air marshal workforce to respond to high threats to aviation. Specifically, according to Secretary Ridge, cross-training immigration and customs officers in air marshal tactics would give DHS greater flexibility to adjust its law enforcement resources according to varying threats and provide a surge capacity during periods of high threats to aviation. The immigration and customs officers would not be used as air marshals during every high-threat period; they would be used as such only when there was a high risk to aviation.

DHS's cross-training plan could have some benefits, but, as we recently reported, it also poses training and administrative challenges.[1] According to the Secretary, the cross-training for immigration and customs agents and Federal air marshals will be centralized. Centralization could eventually produce some cost efficiencies. However, cross-training will expand the roles and responsibilities of all three law-enforcement workforces, and a needs assessment will have to be conducted to identify each workforce's additional training requirements. Cross-training requirements and curriculums will also have to be established and approved. In addition, each affected workforce's organization will have to coordinate the new training requirements with its other mission requirements as it schedules its officers for cross-training. Finally, planned changes in the roles and responsibilities of the Federal law enforcement officers could have implications for their performance evaluations and compensation. Currently, the three law enforcement workforces are under different pay systems and are compensated at different rates. DHS has efforts under way to deal with these issues.

Question 2. Are any new air marshals currently being trained?

Mr. Dillingham's Answer. New air marshals are currently being hired and provided basic training at the rate of about one class per month, a rate sufficient to offset attrition and maintain the current number of air marshals. According to the Federal Air Marshals Service, there is no surge in hiring or training forecasted because the goal for hiring air marshals set by the Secretary of Transportation after September 11, 2001, was met in July 2002, as planned.

In addition to the required basic training, the Service instituted a 4-week advanced training course for air marshals in October 2002. All air marshals hired from October 2001 through July 2002 were required to complete the course by January 2004. Air marshals hired after August 2002 attend this advanced training course after completing their basic training. In August 2003, the Service reported that proposed cutbacks in its training funds would require it to extend the January 2004 date to mid-2004. According to DHS, the Service's transfer to Immigration and Customs Enforcement (ICE) will not adversely affect either the funding for air marshals' training or the schedule for newly hired air marshals to complete the 4-week training course, since a total of $626.4 million is being transferred from TSA to ICE. However, it is not clear how much of the funding will be allocated for training. Given the importance of training to ensure that air marshals are prepared to carry out their mission, we believe that maintaining adequate funding for training should remain a priority.

Question 3. DHS has recently tried to divert $30 million from the Operation Safe Commerce pilot program intended to identify and implement the systemic port security initiation in order to cover a budget shortfall in airport security. Do you believe Federal port security programs are adequately funded?

Ms. Wrightson's Answer. Effective maritime security requires the ability to put preventive systems, controls, and infrastructure in place. According to transportation security experts and state and local government and industry representatives we contacted, funding is the most pressing challenge to accomplishing this task. While some security improvements are inexpensive, most require substantial fund-

[1] U.S. General Accounting Office, *Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed,* GAO–04–242 (Washington, D.C.: Nov. 19, 2003).

ing. Additionally, given the large number of assets to protect, the sum of even relatively less expensive investments can be cost prohibitive. According to Coast Guard estimates, the cost of implementing the new International Maritime Organization security code and the security provisions in MTSA will be approximately $1.5 billion for the first year and $7.4 billion over the succeeding decade. These are substantial sums, but it is not clear at this point how the costs will be paid, as the following examples illustrate.

Funding difficulties can be seen in the implementation of TSA's Transportation Worker Identification Card (TWIC). Although no national estimates of the cost are currently available, they are likely to be substantial. According to a TSA official, nationwide the agency expects to issue five to six million identification cards a year from mid-2004 to the end of 2007. In our work at Los Angeles, port authority officials expressed concern as to how much it may cost to implement this card and all the steps and equipment associated with it, such as the installation of card readers throughout the port, the issuance of cards to port personnel, and adding staff to operate and maintain the system. A study for the ports of Los Angeles and Long Beach estimates that it will cost at least $40 million to perform the necessary start-up tasks. Because of these significant costs, maritime stakeholders are concerned about who will ultimately end up paying for the TWIC. One port authority official indicated that the cost may be passed on to workers as a cost of their employment.

Another example of funding difficulties can be seen at the Federal level, where a MTSA requirement for a vessel identification system is being phased in over time partly because of funding limitations. This identification system, called the Automated Identification System (AIS), uses a device aboard a vessel to transmit a unique identifying signal to a receiver located at the port and to other ships in the area. This information gives port officials and other vessels nearly instantaneous information about a vessel's identity, position, speed, and course. Such a system would provide an "early warning" of an unidentified vessel or a vessel that was in a location where it should not be. MTSA requires that vessels in certain categories[2] install tracking equipment between January 1, 2003, and December 31, 2004, with the specific date dependent on the type of vessel and when it was built. Effectively implementing the system requires considerable land-based equipment and other infrastructure that is not currently available in many ports. As a result, for the foreseeable future, the system will be available in less than half of the 25 busiest U.S. ports.[3]

Installing AIS at the remaining ports depends in part on when funding will be available. The only ports with the necessary infrastructure to use AIS are those that have waterways controlled by Vessel Traffic Service (VTS) systems.[4] Expanding coverage will require substantial additional investment, both public and private. The Coast Guard's budget request for Fiscal Year 2004 includes $40 million for shore-based AIS equipment and related infrastructure—an amount that covers only current VTS areas. According to a Coast Guard official, wider-reaching national implementation of AIS would involve installation and training costs ranging from $62 million to $120 million. Also, the cost of installing AIS equipment aboard individual ships averages about $10,000 per vessel, which is to be borne by the vessel owner or operator. Some owners and operators, particularly of domestic vessels, have complained about the cost of equipping their vessels.

As I suggested in my testimony, where the money will come from to meet these funding needs is not clear. One theme we have heard from maritime stakeholders is that the current economic environment makes this a difficult time for the private industry or state and local governments to make security investments. According to industry representatives and experts we contacted, most of the transportation industry operates on a very thin profit margin, making it difficult to pay for additional security measures. In addition, nearly every state and local government is facing a large budget deficit for Fiscal Year 2004. For example, the National Governors Association estimates that states are facing a total budget shortfall of $80 billion this upcoming year. Given the tight budget environment, state and local governments

---

[2] All vessels of certain specifications on international voyages; self-propelled commercial vessels 65 feet or more in length; towing vessels 26 feet or more in length and more than 600 horsepower; vessels of 100 gross tons or more carrying one or more passengers for hire; and passenger vessels certificated to carry 50 or more passengers for hire.

[3] In addition to Los Angeles/Long Beach, the other ports that currently have this system are New York/New Jersey; the mouth of the Mississippi River; New Orleans; Houston/Galveston; Port Arthur, Texas; San Francisco; Seattle/Tacoma; Alaska's Prince William Sound; and Sault Ste. Marie, Michigan.

[4] Similar to air traffic control systems, VTS uses radar, closed circuit television, radiophones, and other technology to allow monitoring and management of vessel traffic from a central shore-based location.

and transportation operators must make difficult tradeoffs between transportation security investments and other needs, such as service expansion and equipment upgrades. According to the National Association of Counties, many local governments are planning to defer some maintenance of their transportation infrastructure to pay for some security enhancements. At the same time however, the Federal Government faces its own challenges in finding considerable additional funding. Due to the costs of security enhancements and the transportation industries' and state and local governments' tight budget environments, the Federal Government is likely to be viewed as a source of funding for at least some of these enhancements. While Federal monies have been made available, requests for Federal funding for transportation security enhancements will likely continue to exceed available resources given the constraints on the Federal budget as well as competing claims for Federal assistance.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED TO GERALD L. DILLINGHAM

Question 1. I am interested in whether we have enough screeners in place to facilitate the efficient AND secure movement of passengers through the airport security systems. I understand that TSA has recently reduced its screener workforce by 6,000. Could you tell us if the airports and representatives of airports with whom you recently spoke had any thing to say about the situation at airports with regard to whether they had an adequate screening workforce? In GAO's opinion, what would be the right number of screeners at an airport?

Answer. According to airport representatives, their needs are not being matched with the number of available screeners. Some airports maintain they have too many screeners, while other airports say they do not have enough screeners. Airport representatives argue that across-the-board reductions do not necessarily take into account operational issues at airports, such as peaks and valleys throughout the course of the day or week. In addition, seasonal demands, such as summer vacation travel, and demands at airports in certain localities, such as Florida and Nevada, need to be considered.

We do not know the "right" number of screeners, but that number should be based on the operational needs of airports and assume the use of part-time screeners. In addition, the number of screeners needed at individual airports can be expected to change as explosives detection systems (EDS) are integrated with airport baggage-handling systems and used instead of explosives trace detection equipment to screen checked baggage. Because EDS require fewer screeners than trace equipment, less manpower will be needed as more EDS are placed in service.

Question 2. What is the *short* list of actions that you believe must still be taken in the area of aviation security and TSA?

Answer. We believe the following actions still need to be taken in the area of aviation security:

- *Further develop a strategic plan and continue implementation of a risk-based management approach:* As aviation security is viewed in the larger context of transportation and homeland security, and new potential threats emerge daily, TSA needs adequate tools to ensure that its efforts are appropriately focused, strategically sound, and achieving expected results. As we have recommended, it will be important for TSA to set priorities using a risk-based approach so that its resources can be focused and directed to those aviation security enhancements most in need of implementation. TSA is currently developing the National Transportation System Security Plan, which is designed to be a comprehensive security strategy for the transportation system.
- *Share and use intelligence information:* No technology can outperform the use and sharing of intelligence information. It is important to identify and handle terrorists and threats before they come into the country.
- *Address funding issues:* Securing aviation and other critical infrastructure is turning out to be much more costly than originally thought, and the Congress is faced with demands for additional Federal funding for transportation security that far exceed the funds that might be available through the traditional processes. Funding approaches may include (1) better management of available resources and improved accountability systems—including general cost accounting systems and contract management and improved communications with Congress and aviation stakeholders on changing funding needs—and (2) the use of innovative financing options, such as letters of intent and an aviation security capital fund.

- *Accelerate the development and use of security technologies:* When faced with vast and competing demands for security resources, it will be important for TSA to continue its efforts to identify technologies, such as next-generation passenger and baggage screening technologies that will leverage its resources and potentially improve its capabilities.
- *Improve coordination and communication between TSA and airports/local law enforcement:* The development of effective, collaborative relationships between airports, local emergency management agencies, and law enforcement is important to coordination and communication. Key to improving coordination between TSA and airports is establishing clearly defined roles for airport operators and Federal security directors, who are responsible for ensuring that standardized security procedures are implemented at the Nation's airports.

Question 3. In your testimony, you describe the challenge of coordination and communications among different aviation stakeholders. I'm concerned about this, especially in regards to intelligence sharing. I'm concerned about the level of intelligence that is being shared among Federal agencies, which was an identified weakness in our security prior to 9/11. You note in your testimony that GAO has examined the status of terrorist watch lists. What were your key findings in this area with regard to the development of an integrated database of CIA, FBI, DOD and other government agencies with potential terrorist connections?

Answer. In reviewing 12 watch lists maintained by nine Federal agencies, we found that information was being shared among some of them but not among others.[1] Moreover, even when sharing was occurring, costly and overly complex measures had to be taken to facilitate it. To promote better integration and sharing of terrorist and criminal watch lists, we recommended that the Department of Homeland Security, in collaboration with other departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the Federal Government's watch list structures and policies. We recommended that this collaborative effort include:

- updating the watch-list information that we reported on to develop an architectural understanding of the Nation's current watch-list environment;
- defining the requirements of the future consolidated (or "target") watch list's architectural environment, including requirements that address any agency-unique needs that can be justified;
- basing the target architecture on the achievement of the mission goals and objectives contained in the President's homeland security strategy and on congressional direction, as well as on opportunities to leverage state and local government and private sector information sources;
- developing a near-term strategy for implementing the target architecture that provides for the integration of existing watch lists, as well as a longer-term strategy that provides for migrating to a more consolidated and standardized set of watch lists;
- ensuring that these strategies provide for defining and adopting more standardized policies and procedures for watch-list sharing and addressing any legal issues affecting, and cultural barriers to, greater watch-list sharing; and
- developing and implementing the strategies within the context of the ongoing efforts of each of the collaborating departments and agencies.

In addition, as we reported earlier this year,[2] representatives of numerous state and local governments and transportation industry associations indicated that the general threat warnings received by government agencies are not helpful. Rather, they said, transportation operators, including airport operators, want more specific intelligence information so that they can understand the true nature of a potential threat and implement appropriate security measures. In our recent interviews with airport representatives, they stated that intelligence information generated at the local level can differ from intelligence information that is received from the Federal level. Airport representatives are concerned because there is currently no system to reconcile these differences in intelligence information. In addition, airport operators said that it is difficult to assess what is "actionable intelligence."

---

[1] U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing,* GAO–03–322 (Washington, D.C.: Apr. 15, 2003).

[2] U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges,* GAO–03–843 (Washington, D.C.: June 30, 2003).

Question 4. I have heard various opinions about the vulnerability associated with general aviation. On one hand, I have heard it argued that it is a vulnerability because terrorists could use these types of aircraft to deliver a dirty bomb or spread a chemical or biological agent. On the other hand I have heard that the GA community has significantly enhanced GA security since 9/11. What does GAO see as the nature and scope of potential vulnerabilities for general aviation?

Answer. General aviation is vulnerable because general aviation pilots and passengers are not screened before takeoff and the contents of general aviation planes are not screened at any point. General aviation includes more than 200,000 privately owned airplanes, which are located in every state at more than 19,000 airports. More than 550 of these airports also provide commercial service. In the last 5 years, about 70 aircraft have been stolen from general aviation airports, indicating a potential weakness that could be exploited by terrorists. This vulnerability was demonstrated in January 2002, when a teenage flight student stole and crashed a single-engine airplane into a skyscraper in Tampa, Florida. Moreover, general aviation aircraft could be used in other types of terrorist acts. It was reported that the September 11 hijackers researched the use of crop dusters to spread biological or chemical agents.

Since September 11, 2001, the general aviation community, in concert with TSA, has taken several steps to increase security. These steps include the development and publication of plans like *General Aviation Security Best Practices* by the New York State Department of Transportation. Most steps have been voluntary, and no mechanism is in place to ensure that these actions are effective or being implemented.

Question 5. Your testimony states that advancements such as CAPPS II and a trusted traveler program could make screening more efficient. How? Are these programs key to improvements in the screening process? What are the hurdles that need to be overcome to move these programs further along?

Answer. TSA initiatives, such as the next-generation Computer-Assisted Passenger Prescreening System (CAPPS II) and registered traveler program, can improve security by "making the haystack smaller" when looking for the needle (*i.e.,* the terrorists). CAPPS II would use national security and commercial databases to identify passengers who could pose risks for additional screening. Under a registered traveler program, those who voluntarily apply to participate in the program and successfully pass background checks would receive a unique identifier or card that would enable them to be screened more quickly. These initiatives have the potential to be important aspects of the screening process by enabling TSA to focus its limited resources where they will have the greatest impact.

TSA faces a number of challenges that could impede its ability to begin implementing CAPPS II in the fall of 2004, as called for in its current plans. Among the most significant are the following:

- concerns about travelers' privacy rights and the safeguards established to protect passenger data;
- the accuracy of the databases being used by the CAPPS II system and whether inaccuracies could generate a high number of false positives and erroneously prevent passengers from boarding their flights or delay passengers;
- the length of time that TSA will retain data;
- the availability of a redress process through which passengers could get erroneous information corrected;
- concerns that identify theft, in which someone steals relevant data and impersonates another individual to obtain that person's low-risk score, may not be detected and thereby negate the security benefits of the system; and
- obtaining the international cooperation needed for CAPPS II to be fully effective, since some countries consider the passenger information required by CAPPS II as a potential violation of their privacy laws.

In a previous report,[3] we identified key policy and implementation issues that would need to be resolved before a registered traveler program could be implemented. Such issues include:

- the criteria that should be established to determine eligibility to apply for the program;

[3] U.S. General Accounting Office, *Aviation Security: Registered Traveler Program Policy and Implementation Issues,* GAO–03–253 (Washington, D.C.: Nov. 22, 2002).

- the kinds of background checks that should be used to certify applicants' eligibility to enroll in the program and the entity who should perform these checks;
- the security-screening procedures that registered travelers should undergo and the differences between these procedures and those for unregistered travelers; and
- concerns that the traveling public or others may have about equity, privacy, and liability.

Question 6. Your testimony states that Federal Security Directors are the lynchpin of TSA's efforts to coordinate with airports and local law enforcement, but you also allude to some coordination problems out in the field. What's going on, and what can we do to make things better?

Answer. According to aviation stakeholders, cooperation between airport operators and Federal security directors (FSD) has been improving, but the level of coordination varies across airports. Our recent discussions with airport representatives indicated that cooperation and coordination often depend on good working relationships, based in large part on a clear understanding of respective roles and responsibilities, between individual airport operators and FSDs. While some relationships have been successful, others are not working well, according to airport representatives. For example, one FSD directed an airport to implement TSA guidance that contradicted the airport's security plan, which TSA had approved. This situation was confusing for the airport operator. One potential fix is additional training to ensure that all FSDs are uniformly implementing TSA policies.

Question 7. GAO has done a significant number of studies and analyses related to human capital issues across the Federal Government as well as looking at TSA in particular. Now that the agency and its staff are in place, we are moving more into the area of sustainability and institutionalizing a high-performance organization. What does GAO think are the challenges for TSA as it moves into its next phase of development and what do you think of TSA's efforts to date to meet those challenges?

Answer. TSA faces the challenge of strategically managing its workforce of more than 60,000 people to ensure that this new and relatively inexperienced workforce expands its skills and becomes a world-class security workforce. This effort will entail the establishment of a screener performance management system so TSA will know where to concentrate its training efforts. Additionally, over the next several years, TSA faces the challenge of "right-sizing" this workforce as efficiency is improved with new security-enhancing technologies, processes, and procedures. For example, as explosives detection systems are integrated with baggage-handling systems, the use of more labor-intensive screening methods, such as trace detection techniques and manual searches of baggage, can be reduced. Other planned security enhancements, such as CAPPS II and the registered traveler program, also have the potential to make screening more efficient.

In January 2003, we reported [4] that TSA was addressing some critical human capital success factors by hiring personnel, using a wide range of tools available for hiring, and beginning to link individual performance to organizational goals. However, concerns remain about the size and training of the screener workforce, the adequacy of the initial background checks for screeners, and TSA's progress in setting up a performance management system. The next steps are for TSA to clearly define the roles and responsibilities of its various offices, provide training for supervisors and managers to ensure that they are capable supervisors, and continue workforce planning efforts to have the right number and mix of staff. As a step in that direction, TSA is currently developing a human capital strategy, which it expects to be completed by the end of this year.

Question 8. In your testimony before our aviation subcommittee in April of this year, you told us that in FY 2002 over half a billion dollars of AIP money had been used for aviation security and had resulted in some airport capacity projects going unfunded. Your testimony today again raises the issue of how we can fund needed security projects and maintain and expand the system's capacity. In your testimony, you state that one of the key challenges in aviation security is paying for it. This concerns me, as AIP money is supposed to go towards other airport development projects. How can we adequately fund aviation security without such a great reliance on AIP money?

---

[4] U.S. General Accounting Office, *Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture,* GAO–03–190 (Washington, D.C.: Jan. 13, 2003).

Answer. As we previously reported to this committee,[5] consideration should be given to establishing a dedicated and predictable source of funds for aviation security. Proposed aviation reauthorization legislation would establish an aviation security capital fund that would authorize $2 billion over the next 4 years. This funding would be made available to airports in letters of intent, and airports would be expected to provide a match of either 5 or 10 percent of a project's costs. This proposed capital fund could minimize the need to use AIP funds for security projects. We also identified letters of intent as a funding option that has been successfully used to leverage private sources of funding. TSA has since signed letters of intent covering seven airports—Boston Logan, Dallas/Fort Worth, Denver, Los Angeles, McCarran (Las Vegas), Ontario (California), and Seattle/Tacoma. Airport representatives said that about 30 more airports have requested similar agreements.

Question 9. I see from your testimony today that you solicited the aviation security concerns and issues of some of the principal stakeholders in the aviation community including representatives of the airports, airlines and the general aviation community. Could you share with us some of what you heard about their key concerns and issues?

Answer. Key issues raised by aviation stakeholders include the following:

- *Coordination*—During our discussions, stakeholders noted that coordination at the local level depends, in large part, on the relationship between the Federal security director and the airport operator. Some stakeholders also said that TSA does not work with them early in the decision-making process and only informs them of decisions after the decisions have been made. According to the stakeholders, this lack of coordination leads to confusion and resentment, along with policies that are difficult to enforce operationally, because the policies have been created without any input from the airport operators. In addition, this process can be costly. For example, TSA may decide on a policy without receiving any input from stakeholders and then have to change the policy because the airports find the policy unworkable.
- *Funding*—Stakeholders noted funding as a major issue. Airports are concerned about the high price of terminal modifications for explosives detection systems and other security improvements. In addition, airlines are concerned that the addition of passenger security fees may lead to fewer people flying, at a time when the industry is experiencing economic hardship.
- *Hassle Factor*—Stakeholders are concerned about the "hassle factor," or the perception of it. For example, stakeholders told us that long lines at security checkpoints discourage the public from flying and reduce the number of "short haul" trips and business travelers, thereby reducing the airlines' income.
- *General Aviation*—Industry representatives are concerned that information about general aviation security and its vulnerabilities is not based on intelligence data or accurate information. For example, representatives said that although there are a number of general aviation aircraft located near nuclear power plants, a small general aviation plane could not damage a plant. Stakeholders from the general aviation community told us that they would like to see a risk-based plan that addresses general aviation security, including an evaluation of the threats, vulnerabilities, and criticalities of general aviation.

Question 10. The expansion of the Federal Air Marshal Service is one of the enhancements that were initiated after the attacks of 9/11. Since that time, I have seen several stories in the national media that could lead one to believe that the service is in total disarray and raise some serious questions as to whether the service can adequately fulfill its mission. I see from your testimony that you have a study of the Federal Air Marshal Service underway. Could you tell the Committee what issues you are focusing on in your study and when you expect to have a report? Will you be looking at the effect of moving the FAMs out of the TSA?

Answer. We are examining the past, present, and future of the Federal Air Marshal Service (the Service). The study examines how the Service has evolved since its post-9/11 expansion, including the extent to which TSA has developed plans and initiatives to sustain the program and accommodate its future growth and maturation. We are also looking at the challenges the Service faces as it moves from the Department of Transportation to the Department of Homeland Security and from TSA to the Bureau of Immigration and Customs Enforcement, as well as the effects of these challenges on its overall sustainability and status as an integral part of the

[5] U.S. General Accounting Office, *Airport Finance: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development,* GAO–03–497T (Washington, D.C.: Feb. 25, 2003).

aviation security system. Within this framework, we are examining whether any activity, including background checks and training, compromised aviation security and the Service's ability to carry out its mission. In addition, we are looking at the adequacy of efforts to rectify any problems that surfaced. We expect to issue our report on this work at the end of November.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN MCCAIN TO MARGARET WRIGHTSON

Question 1. In your written statement, you identify 5 issues that bear watching. Could you briefly describe the ones you see as most important and how they impact port security? What future oversight or actions would you see as needed in these areas to ensure that MTSA is effectively implemented and achieves the results Congress intended?

Answer. The issues we identified, while separate and distinct, share two common themes related to solving them and ensuring that MTSA is implemented effectively. Given the limited resources that are available relative to the needs that exist, attention to both of these matters is important.

- *Need for cost-conscious project design and management.* Several important considerations need to be kept in mind. First, DHS and the Coast Guard should avoid putting money into duplicative efforts unless there is a compelling business case for doing so. Intelligence is one area where we already have identified the potential for duplication; the Port Security Assessment program (discussed further under question 2 below) certainly represents another. Second, DHS cannot afford to subsidize activities and improvements that could be readily supported by other means. Making sure that TSA enforces matching requirements for future port security grants is one example of how to avoid such subsidies. Third, where new security processes and technologies are being put into place, it is worth considering whether there might be innovative approaches for sharing costs or operations. For example, to implement MTSA's automatic identification system (AIS) requirement for a system that identifies and tracks vessels entering key ports, expensive new infrastructure will be needed at a number of ports. One model worth considering is the one already in place at the ports of Los Angeles and Long Beach, where the cost for both the infrastructure and ongoing operations of a vessel traffic service system was shared between the Coast Guard and local and state sources.
- *Use of risk management in decisionmaking.* Risk management is important for decisionmaking because of the difficult trade-offs the government will likely have to make as it moves forward with its security efforts. Ports will always be at risk to some degree, but the risk can be reduced. Since spending is already constrained by budget limitations, it is important to spend as wisely as possible for efforts to reduce the risk to ports. Under a risk management approach, for example, decisions would be based both on the nature of the threat, the vulnerability of an asset at a port, and the criticality (that is, the relative importance) of the asset. Infrastructure that is both critical and highly vulnerable would be a high priority for funding. By comparison, infrastructure that is vulnerable to attack but not as critical, or infrastructure that is very critical but already well protected, would be lower in priority. The importance of such an approach merits continued congressional attention to whether the cognizant agencies are using it adequately and appropriately.

Finally, at this early stage of the process, it is difficult to be certain that the key issues have surfaced. Partly for this reason, a number of GAO engagements, requested by this Committee and others in Congress, are still ongoing. Further oversight may be needed in the future—for example, after the June 30, 2004, implementation deadline for security plans and the December 31, 2004, deadline for AIS. Other programs with longer-term implementation schedules, such as the Transportation Worker Identification Credential (TWIC), may require additional regular oversight.

Question 2. You note in your written statement that GAO has concerns about the Port Security Assessments now under way at the Coast Guard. What do you think the Coast Guard needs to do to fix this problem?

Answer. The Coast Guard and its contractor should take several actions to improve the Port Security Assessment program. First, to incorporate knowledge gained from the pilot assessments in Huntington and Tampa, the Coast Guard should not start any additional port security assessments until the two pilots have been completed. Second, rather than comprehensively reassess facilities for which security as-

sessments have previously been completed, the Coast Guard should review these assessments, identify gaps, and supplement them as needed. In this regard, the Coast Guard should give leading roles to its Port Security Assessment Team and its Captains of the Port in deciding what facilities or infrastructure need to be assessed, because these officials have the necessary expertise and experience to decide which work will add the most value to what is already known about security at the port. Third, to reduce the burden on port stakeholders and encourage their participation, the Coast Guard and its contractor should be more careful about limiting information requests to security-related matters. Third, Such actions would reduce the burden on stakeholders and save money and time. Finally, to ensure the quality and accuracy of the final assessment report, the Coast Guard should incorporate a quality review into the report drafting process. This action provides an opportunity for stakeholders to review the draft for accuracy. We are in discussions with the Coast Guard on these matters, and they have indicated they are in the process of making changes to correct the problems.

Question 3. It's troubling to read in your statement that two years after September 11 we will not have AIS coverage in 25 of the busiest ports in America. What is the problem here, and what will it take to solve it?

Answer. The main problem is one of insufficient infrastructure at about half of the 25 ports, and solving it will take both money and time. AIS is a shipboard device that transmits identity and location information via radio broadcast as frequently as every two seconds, both ship-to-ship and ship-to-shore. This allows persons both on shore and aboard each ship to identify vessels and track their position. According to the Coast Guard, only 10 ports with Vessel Traffic Service (VTS) systems will have the infrastructure in place to implement AIS by December 31, 2004; ports without existing VTS service will require additional time and investment to develop the necessary infrastructure. [This additional infrastructure includes transmission towers, control rooms, and equipment for receiving and transmitting radio signals. The cost of this infrastructure will likely run into the millions of dollars at each port.] Expanding coverage will also require the installation of AIS technology on substantially more vessels and hence additional private investment. Additionally, legal questions pertaining to licensing of radio frequencies needed to operate AIS in some areas may need to be resolved.

The absence of AIS at a port does not mean that the port is unprotected. All ports, including those that will not have AIS implemented by December 31, 2004, are protected by several layers of defense. For example, vessels coming into U.S. ports must provide 96-hour advance notice of arrival, sensitive facilities in ports are surrounded by security zones that preclude intrusion by unauthorized vessels, and the U.S. Coast Guard and other security organizations patrol waterways in the ports. Local port control by harbormasters can also monitor vessels traffic in and out of ports.

Question 4. Which agency within DHS is the lead agency on maritime security? Which agency do you believe is best equipped to take the lead role in maritime security?

Answer. The Coast Guard is currently the lead agency for maritime homeland security, while the Navy has primary responsibility for maritime homeland defense. The Coast Guard has historically performed the maritime homeland security role, and it—more than any other agency within DHS—has the resources, expertise, and legal authority to continue in this capacity. While our work in this area is ongoing, we have not identified other organizations or entities better situated to take the lead role in accomplishing the mission of maritime homeland security. However, the Coast Guard needs to keep two main considerations in mind as it exercises this responsibility:

- *Need to balance this role with other missions.* It is clear that the Coast Guard is facing daunting challenges to fulfill these new responsibilities while also meeting its other missions. As we testified last spring, there were two missions in which the Coast Guard's level of effort (as measured by resource hours spent using cutters, boats and aircraft) were significantly below historical levels. These were drug interdiction (down by about two-thirds between the first quarter of 1998 and the first quarter of 2003) and fisheries enforcement (down about one-third for the same period). The Coast Guard's alignment of missions has been an area of much congressional concern, and the Coast Guard has been tasked with developing a strategy that outlines how it sees its resources—cutters, boats, aircraft, and personnel—being distributed across all of its various missions, as well as a time-frame for achieving the desired balance among missions. The Coast Guard is currently working on this plan but has not yet completed it.

- *Need for coordination across all of DHS.* Although the Coast Guard has lead responsibility for maritime security, it cannot or should not go it alone in isolation from other DHS Directorates or offices. As we have testified, for an effective maritime security strategy to be developed and implemented, it is critical that the Coast Guard and the other agencies folded into DHS deal effectively with a myriad of organizational, human capital, process, technology, and environmental challenges. Because we recognize the difficulty of this enterprise while also working to maintain readiness, we have designated the implementation and transformation of DHS—including those aspects pertaining to the Coast Guard—as a high-risk area.