U.S. Senate Committee on Governmental Affairs Pre-hearing Questionnaire
For the Nomination of Admiral David Stone to be
Assistant Secretary of Homeland Security,
Transportation Security Administration

I. Nomination Process and Conflicts of Interest

1. Why do you believe the President nominated you to serve as Assistant Secretary of Homeland Security, Transportation Security Administration (TSA)?

Answer: I am grateful for the trust and confidence that the President has shown in me by nominating me to this important position. As a United States Naval Officer for almost 28 years I achieved the rank of Rear Admiral and during my career was responsible for commanding sailors and marines and entrusted with billions of dollars of valuable military equipment. More importantly, I played a key role in the defense of the strategic interests of the United States. I believe that these are qualities that the President looked favorably on. In both the Navy and at TSA I have successfully managed and led large organizations. I was one of the first Federal Security Directors named by Secretary Mineta shortly after TSA was stood up as an agency and I served as the first Federal Security Director at Los Angeles International Airport (LAX). At LAX, I undertook and met the challenge to maintain security as the airport transitioned from the pre-9/11 screener staff to a new, federalized and highly trained workforce. I met two critical statutory deadlines at LAX, one of the busiest airports in the nation and the world. As the Acting Administrator for TSA since December 2003, I have guided TSA as it has continued to improve its ability to provide for security in all modes of transportation.

2. Were any conditions, expressed or implied, attached to your nomination? If so, please explain.

Answer: There were no conditions, expressed or implied, attached to my nomination. I have been asked to lead TSA in accordance with law and regulation.

3. What specific background and experience affirmatively qualifies you to be Assistant Secretary of Homeland Security (TSA)?

Answer: My leadership skills, developed during a lifetime of service to this country, enable me to successfully lead TSA. I understand our Nation's homeland security organization and how transportation security factors into it. I am committed to a full partnership with the many stakeholders in the transportation sector, including state and local governments, Indian tribes, private industry, and the American public, all of which rely heavily on a secure transportation system. I am working closely with Members of Congress to ensure TSA remains focused on preserving our freedoms while we go about our important work of protecting America.

4. Have you made any commitments with respect to the policies and principles you will attempt to implement as Assistant Secretary? If so, what are they and to whom have the commitments been made?

Answer: I have made no commitments other than to continue to ensure that TSA, its thousands of employees, and its supporting contractors, do their utmost to provide for effective security across the transportation sector, while providing world-class customer service, and ensuring the freedom of movement of people and commerce. I have pledged to make TSA more responsive to the customer needs on the local level by empowering our Federal Security Directors with more authority and responsibility. If confirmed, I will have a senior role within the Department of Homeland Security and I will do my utmost to work effectively with the President, Secretary Ridge, Deputy Secretary Loy, Under Secretary Hutchinson and other senior Department leaders, as well as with the Congress, to continue to protect the homeland.

5. If confirmed, are there any issues from which you may have to recuse or disqualify yourself because of a conflict of interest or the appearance of a conflict of interest? If so, please explain what procedures you will use to carry out such a recusal or disqualification.

Answer: There are no issues that I can currently foresee affecting TSA that will require me to recuse or disqualify myself because of a conflict of interest or the appearance of a conflict of interest. However, should a situation arise that calls this into question, I will immediately consult with the Department's Designated Agency Ethics Official to seek advice and guidance.

II. Role and Responsibilities of Assistant Secretary of Homeland Security (Transportation Security Administration)

6. What is your view of the role of Assistant Secretary of Homeland Security (TSA)?

Answer: The key role of the Assistant Secretary of Homeland Security (TSA) is to provide Leadership in the ongoing effort to protect the US Transportation Sector against a terrorist attack. In addition to providing leadership (leading people, leading technology, leading change), it is important that the Assistant Secretary also promotes a spirit of Partnership with all entities involved in the protection, operation, and use of the Transportation Sector. Strong partnerships are one of the keys to success in the War on Terror. Finally, building Friendships is also of great importance. These Friendships are all about building a foundation of "Trust and Confidence" with the American People. By respecting Individual Privacy and performing the TSA's mission with a high level of Customer Service, a level of friendship with the American people is formed which reinforces the notion that as "friends" we are all engaged in a common struggle to protect America against the threat of Terrorism. In summary, fostering the concepts of Leadership, Partnership and Friendship within the Transportation Sector are all roles the Assistant Secretary should be executing each day.

7. In your view, what are the major internal and external challenges facing TSA? What do you plan to do, specifically, to address these challenges?

Answer: Internal challenges to TSA include: (1) Enhance operational field focus and establish inter-modal risk mitigation planning. (2) Cut layers of HQ staff between the Administrator and the field. (3) Empower the Federal Security Director (FSD) and allow for more local decision-making. (4) Make the concept of a Model Workplace for TSA employees a reality. (5) Accelerate deployment of technology to the field and reduce the dependence on the high number of personnel that are currently needed to provide security.

Actions to address these internal challenges include: (1) Conduct daily operation and intelligence briefings with Senior staff utilizing the Transportation Security Operations Center as the TSA operational center of gravity. (2) Realign the TSA HQ Staff to provide for better integration and to reduce the layers between the Administrator and the field. (3) Initiate action to allow for local testing, local training, and local hiring in order to facilitate the empowerment of the Federal Security Director in the field. (4) Constantly review issues that impact the morale and welfare of TSA employees and ensure leaders are held responsible for taking measures to enhance the Quality of Life and Quality of Work of each TSA employee. (5) Develop Transition plans to accelerate deployment of technologies to the field that enhance security and reduce both the number of personnel and the level of effort required to perform the security mission.

External challenges for TSA include: (1) Integrating fully within the Department of Homeland Security in order to operate most effectively and efficiently. (2) Developing thoughtful Protection Plans for the Transportation and Shipping and Postal critical infrastructure sectors in partnership with other entities to more fully mitigate the risk of Terrorist attack. (3) Ensuring the Privacy and Freedoms we all enjoy as Americans are preserved as we seek out innovative ways to better protect America against a Terrorist attack. (4) Accelerating the use of technology to enhance the transportation security.

Actions to address these external challenges will include: (1) Imbue within TSA a culture of change to drive out concepts such as "protecting turf." Constantly seek to integrate TSA activities within DHS to get the maximum use of every tax dollar. (2) Partner with other government agencies and the private sector in developing Protection Plans for the Transportation and Shipping and Postal critical infrastructure sectors. (3) Constantly review privacy issues to ensure actions are taken in a proactive manner to protect our freedoms as we carry out the TSA mission. (4) Develop transition plans for technology that can facilitate the smooth flow of commerce while enhancing the security of the overall process. The use of new technology to reduce the level of personnel needed to carry out a specific task can in many cases allows for a more efficient and effective use of the taxpayers dollar.

8. How do you plan to communicate to the TSA staff on efforts to address relevant issues?
Answer: I am very proud of the internal communications procedures that we already have in place that allow me, as the Acting Administrator, to communicate with TSA staff

on important matters. We have a number of communication vehicles in place, including: the TSA employee newsletter the *Sentinel*, letters from the Acting Administrator to employees in the *Sentinel*, an extensive Intranet (section on *What Others are Saying About TSA* and *Things To Know, Things to Share*), Extranet (password protected internal site on the public domain), broadcast messages to all TSA employees, TSA training, a message of the week, TSA Employee Open House, Brown Bag Luncheons, and Town Hall meetings. If confirmed, I will continue to use these vehicles to communicate important information to TSA staff.

III. Policy Questions

GENERAL

9. GAO as well as the DHS IG and others have identified a number of long-term management and organizational challenges TSA faces to sustaining enhanced aviation security that include paying for increased aviation security needs and controlling costs and establishing effective coordination among the many entities involved in aviation security.

a. How can TSA most effectively control the costs of aviation security needs?

TSA works to control the costs of aviation security needs by addressing external factors in conjunction with our stakeholders in the aviation industry and ensuring that TSA is effectively using the funds we receive.

As I expressed earlier in my response to Question 6, the concepts of Leadership, Partnership and Friendship are critical in building a consensus among all transportation providers, including of course the aviation industry. I apply these precepts in dealing with external organizations, which cut across the aviation spectrum. Security requirements that TSA issues and enforces affect airport operators, the air carriers (passenger and all-cargo), aviation manufacturers, State and local law enforcement, General Aviation pilots, direct and indirect air cargo shippers and freight forwarders, commercial businesses operating at airports serving passengers and air carriers, airline passengers, and employees of airports and air carriers, to name just some of them. As part of our rule making process, TSA must put its proposed security requirements through a rigorous economic analysis, except in emergency situations. The rule making process is an open one that invites substantial comment from the public, including of course parties that are directly impacted by the regulations. This assures that any costs imposed on industry or the public have been fully vetted and justified. We fully understand that if we make air travel and commerce prohibitively expensive then the terrorists will have won.

TSA also collects security fees as directed in ATSA . The funds we collect reduce the amount of appropriations TSA receives from the General Fund for aviation security

needs. As stewards of the public purse on this matter, TSA is responsible for ensuring that air carriers accurately forward the passenger and carrier fees to TSA. Internally, TSA has a rigorous program of controls to ensure that appropriated funds are properly spent. Our Chief Financial Officer leads the effort to effectively manage TSA resources. We have had our financial systems audited by the DHS Inspector General, and they received a clean audit opinion. TSA relies heavily on contractor support for functions that in many long established agencies are handled in-house. This allows us to concentrate on our core functions of providing transportation security in a reliable and cost effective manner. As a result of this reliance on contractor support, TSA also has a vigorous complement of staff overseeing these contracts to again ensure that we are receiving our money's worth.

b. What further steps, if any, should be taken to increase coordination among the many entities involved in aviation security?

Answer: While TSA has a central role in aviation security, effectively securing our nation's aviation system can only be accomplished in partnership with relevant Federal, state, tribal, local and private industry entities. TSA coordinates the efforts of these partners, under the guidance of the Secretary and the Under Secretary for Border and Transportation Security. As part of its coordination responsibility, TSA identifies gaps and works with appropriate partners to ensure those security gaps are filled.

TSA also coordinates work on the Transportation Sector Specific Plan, as part of the National Critical Infrastructure Protection Plan, which will identify Federal and private-sector stakeholders in the sector, their roles and relationships and their means of communication. This effort will facilitate coordination among the many entities involved in aviation security.

10. GAO, the DHS IG and others have identified other long-term management and organizational challenges including developing and implementing a comprehensive risk management approach and strategically managing its workforce.

a. What is the role of TSA in identifying threats, vulnerabilities, and criticalities of the nation's transportation infrastructure? What changes should be considered in enhancing this role?

Answer: The Department has instituted a risk management approach to protecting our nation's critical infrastructure, under the leadership of the Information Analysis and Infrastructure Protection directorate. TSA works within this framework looking particularly across the modes of transportation to identify security gaps and strategies to ensure consistency in security response that takes into consideration inter-modal issues (such as assets, incidents, or supply chains that straddle multiple modes, and inter-modal exercises).

More specifically, Homeland Security Presidential Directive 7 (HSPD-7) directs the establishment of "a national policy for Federal departments and agencies to identify and

prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." This effort includes development of the National Infrastructure Protection Plan under DHS leadership. The plan includes Sector Specific Plans (SSPs), and TSA has been assigned primary responsibility for developing the Transportation SSP.

In developing the Transportation SSP, TSA is working under BTS guidance and partnering with the U.S. Coast Guard, other BTS component agencies and the Department of Transportation (DOT) modal administrations. The plan, which is being developed, will identify Federal and private-sector stakeholders in the sector, their roles and relationships and their means of communication; how important assets in the transportation sector will be identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured; and how research and development will be prioritized in the sector. In the Transportation Sector, the SSP will further efforts currently underway and help ensure that they are systematic, complete, and consistent with the efforts in the other 12 sectors.

b. Since TSA began operations, much of the agency's attention and resources have been focused on securing passengers and baggage at the nation's commercial airports. As the agency moves forward, what is the appropriate balance between focusing on aviation security and security for other modes of transportation?

Answer: Much of TSA's activities support our mission across the various transportation modes, making them difficult to categorize as exclusively benefiting a single mode. Although the creation of a Federal screener workforce has meant that TSA currently channels a greater proportion of the security costs for aviation compared to other modes, transportation security is a partnership among Federal, state and local governments and the private sectors. Working with our partners, TSA plays an active role throughout the entire transportation system providing research and development, advisory services, and intermodal coordination. TSA's specific role within each sector will vary from mode to mode. In aviation security, TSA has very specific operational responsibility and the lead regulatory role. In partnership with other DHS components and in coordination with the Department of Transportation (DOT), state, local and private sector partners, TSA's efforts in non-aviation security over the past two years have focused on greater information sharing between industry and all levels of government, assessing vulnerabilities in non-aviation sectors to develop new security measures and plans, leveraging existing security initiatives, increasing training and public awareness campaigns, and providing greater assistance and funding for non-aviation security activities.

Additionally, as TSA continues work on the Transportation Sector Specific Plan and modal plans, as part of the National Critical Infrastructure Protection Plan, TSA will work to identify gaps in security across the modes; how important assets in the transportation sector will be identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured; and how research and development will be prioritized in the sector.

c. What is the appropriate role of the federal government in providing and funding transportation security?

Answer: Ensuring that our nation's transportation systems are secure must be accomplished through effective partnering between appropriate Federal, state, tribal, local and private industry entities. This responsibility must involve the coordination of appropriate Federal, state, tribal, local and private industry partners, many of whom have always been and continue to be in the business of providing security for their particular piece of the transportation sector.

The Department of Homeland Security (DHS) has requested substantial resources in FY 2005 that will improve transportation security in modes other than aviation, including resources in the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) for ports, maritime security, and cargo security; in Information Analysis and Infrastructure Protection (IAIP) for vulnerability assessments, intelligence, and infrastructure protection for all sectors including transportation; and in Emergency Preparedness & Response (EP&R) for emergency response to only name a few. In addition to working with other DHS components, TSA works closely with our sister Federal agencies outside of DHS to ensure that all government resources are maximized. For example, under the leadership of BTS and DHS, TSA is working closely with modal administrations of the Department of Transportation to help leverage their existing resources and security efforts to accomplish unified security goals.

In developing the Transportation Sector Specific Plan, TSA and its partners will identify Federal and private-sector stakeholders in the sector, their roles and relationships and their means of communication.

d. What portion of security costs should industry bear in comparison to federal, state and local governments?

Answer: Ensuring that our nation's transportation systems are secure must be accomplished through effective partnering among appropriate Federal, state, local and private industry entities. Part of TSA's responsibility is coordination of these entities, many of whom have always been and continue to be in the business of providing security for their particular piece of the transportation sector.

I strongly support the idea that homeland security is a national responsibility shared by all states and localities. That is why I firmly believe that there should be a minimum level of preparedness across the county and that every state should receive some level of assistance from the Department of Homeland Security. The expeditious and efficient award of homeland security funds to states and localities is a primary goal of the Department of Homeland Security. Since its creation last year, the Department has provided more than $8 billion to support and enhance the security of states and localities. The President's Fiscal Year 2005 budget request continues this strong support and commitment to the Nation's emergency prevention and response community. The President's budget clearly demonstrates the continuing priority placed on homeland

security through requesting $40.2 billion in total new resources for FY 2005, which is an increase of 10 percent above the comparable FY 2004 level.

DHS Secretary Ridge has announced the creation of the Office of State and Local Government Coordination and Preparedness (SLGCP) in order to consolidate departmental programs, including grants, and relationships that relate to state and local governments. The consolidation of these programs within SLGCP will eliminate duplication along program lines, enable the complementary and synergistic aspects of these programs to work together, and maximize the effectiveness of federal resources. The Office has several responsibilities, including coordinating the Department's activities with State and local government; assessing and advocating for resources needed by State and local government to implement the national strategy for combating terrorism; providing State and local government with regular information, research, and technical support to assist local efforts at securing the homeland; and developing a process for receiving meaningful input from State and local government to assist the development of the national strategy for combating terrorism and other homeland security activities.

Additionally, Secretary Ridge recently announced a Homeland Security Funding Task Force composed of state, county, city, and tribal representatives to examine the funding process and ensure that Department of Homeland Security funds move quickly to local first responders. The Task Force will identify state and local funding solutions that work effectively and can be extended to situations where there are impediments to the efficient and effective distribution of state and local homeland security funds.

The Task Force is composed of governors, mayors, county officials, tribal leaders and other senior officials with first-hand experience in homeland security issues and will operate under the aegis of the Homeland Security Advisory Council (HSAC) and its State and Local Officials and Emergency Response Senior Advisory Committees. The Secretary will receive recommendations from the Task Force members and the HSAC on how to expedite the money distribution process.

TSA and DHS will continue to work with its Federal, state, local and private industry partners to ensure that we secure transportation to ensure that security costs are appropriately borne by all partners.

11. According to GAO reports and testimony before Congress, TSA has been working on a national transportation system security plan. Admiral Loy testified in May 2003 that TSA was "close to the first draft" of this plan, but this plan has not yet been released.

    a. How has TSA been setting its spending and strategic priorities in the absence of this plan?

Answer: TSA has been spending the majority of its funding and effort as directed by Congress towards what has been the largest and most consistent potential threat, attacks on our aviation system. At the same time, TSA has been working to improve security in other modes of transportation, including building cooperative relationships with our

government partners, such as DOT and the US Coast Guard, and our private sector partners. While the emphasis in aviation has been on a large Federal presence, in the other modes protective activities are being carried out by or in conjunction with the private sector and state, tribal, and local governments who are locally responsible for operations. TSA, under DHS, provides Federal leadership in terms of guidance, assistance and coordination, as seen in the design of protection plans outlined below.

b. When will this plan be completed?

Answer: In December 2003 the President issued Homeland Security Presidential Directive 7 (HSPD-7) that defined the vision for protection of Critical Infrastructure not just in the Transportation Sector, but across the entire national economy. The Department's plan for implementing HSPD-7 involves an overarching National Infrastructure Protection Plan developed by the Information Analysis and Infrastructure Protection Directorate (IAIP), and 17 supporting Sector Specific Plans (SSPs) dealing with the 4 Key Resources and the 13 Sectors such as Transportation. TSA has been assigned to develop the Transportation SSP in conjunction with our partners at DOT and USCG and under the guidance of the Undersecretary for Border and Transportation Security. The first draft of the Transportation SSP is due shortly.

This SSP - and the deep engagement with our partners that developing it has entailed - will accomplish much of what was intended by the original NTSSP referred to in the question. It also has the added benefit of consistency with other sectors and integration into a national economy-wide plan. After the initial rounds of review and integration - estimated to be late summer - TSA will work to expand the essentially complete SSP to include the remaining functions of intended by the original draft NTSSP. Those additional functions include ties to HSPD-5 and the National Response Plan; ties to HSPD-8, preparedness, and exercises; and guidance for developing Modal Security Plans that will go into more detail in each mode. This expanded Transportation SSP should be completed in draft by late fall, and development of the supporting Modal Security Plans should be underway at that time as well. The USCG is already leading development of the National Maritime Security Plan required under MTSA, which will also serve as the maritime Modal Security Plan in the expanded SSP framework.

c. How will TSA integrate other agencies, like the Federal Transit Administration and the Federal Railroad Administration, state and local agencies, and private industry into this planning and standard setting process?

Answer: In the process of developing the HSPD-7 -driven Transportation SSP, TSA has deeply engaged with DOT. In the particular case of FTA and FRA, TSA has worked closely with both agencies in response to the tragic events of March 11 in Madrid and the earlier attack in Moscow. I expect and intend for this close coordination to continue beyond specific high-level planning projects, and beyond response to specific incidents, and to be an ongoing every-day way of doing business. This includes activities in the

realms of detailed security planning; setting standards; and interacting with and getting input from our shared set of state, tribal, local, and private sector stakeholders.

In addition to the senior-staff-level engagement with DOT just described, I have personally engaged the Administrators and Deputies of the Modal Administrations, and I also intend for that to be a regular, ongoing way of doing business.

d. Will TSA provide technical assistance to transportation systems to help them develop their own security plans? If so, will TSA also provide funding for systems that do not have the resources to develop plans?

Answer: TSA's strategic role in securing the transportation system begins at the system or sector-wide level. The strategic priority is to identify security gaps and establish strategies to ensure consistency in security response. Inter-modal issues such as assets, incidents, supply chains that straddle multiple modes, and inter-modal exercises are taken into consideration.

Homeland Security Presidential Directive 7 (HSPD-7) directs the establishment of "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." The Department of Homeland Security (DHS) is responsible under HSPD-7 for developing a National Critical Infrastructure Protection Plan. This plan will be comprised of Sector Specific Plans (SSPs), and TSA has been assigned primary responsibility for developing the transportation SSP.

A first draft of the SSP is due to DHS early this summer (concurrent with the due dates for SSPs from the other 12 sectors of critical infrastructure). In developing the Transportation SSP, TSA is working under BTS guidance and with partners in the U.S. Coast Guard and other BTS component agencies, as well as with the Department of Transportation (DOT) and its modal administrations. The SSP will discuss how Federal and private-sector stakeholders will communicate and work together; how important assets and vulnerabilities in the transportation sector will be identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured; and how R&D will be prioritized in the sector. In the Transportation Sector, the SSP will further these efforts currently underway and help ensure that they are systematic, complete, and consistent with the efforts in the other 12 sectors.

TSA's role within each sector will vary from mode to mode. In aviation security, TSA has the operational and regulatory lead role. TSA's efforts in non-aviation security over the past two years have focused on greater information sharing among industry and all levels of government. The emphasis has been on assessing vulnerabilities in non-aviation sectors, developing new security measures and plans, increasing training and public awareness campaigns, and providing greater assistance and funding for non-aviation security activities. In partnership with other component agencies of DHS and in coordination with DOT, State, tribal, local and private sector partners, TSA will continue to leverage existing security initiatives, coordinate the development of national

performance-based security standards and guidance; identify areas where regulations may be necessary to improve the security of passengers, cargo, conveyances, transportation facilities and infrastructures; and identify areas where better compliance with established regulations and policies can be achieved. TSA will work with DHS components, modal administrators within DOT, and its government and industry stakeholders to continue these efforts, establish best practices, develop security plans, assess security vulnerabilities, and identify needed security enhancements.

TSA has also developed the TSA Self Assessment Risk Model (TSARM). This is designed to assist asset owners/operators in developing a security plan. The tool captures an asset's baseline security posture and identified additional measures that could be undertaken to reduce vulnerabilities. This tool is available at no-cost to users. Currently, a maritime module is operational with development efforts underway for General Aviation and Mass Transit. It is TSA's intent to have modules for each transportation mode.

12. In June 2003, GAO reported that TSA had adopted a "risk management" approach in its efforts to improve U.S. transportation security. (*Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843) GAO described this approach as a process to "analyze threats, vulnerabilities and the criticality ... of assets." Since transportation is a critical asset, and the performance of vulnerability and risk assessments for critical infrastructure is a responsibility of the Directorate for Information Analysis and Infrastructure Protection (IAIP), what role do you expect IAIP to play in conducting this analysis? What is the status of these assessments?

Answer: TSA has been working closely with IAIP's Protective Services Division to coordinate transportation-related risk management efforts. As IAIP develops the list of nationally-critical infrastructures and guidelines therein or under IAIP's guidance as to what signifies critical infrastructure… TSA has supplied IAIP with data pertaining to nationally-critical transportation assets as it is being compiled. Vulnerability assessments completed by TSA are available for IAIP's use. Similarly, TSA receives assessment information conducted by IAIP on transportation-related high value targets. TSA and IAIP work closely to ensure coordination without duplication of efforts.

TSA has developed a vulnerability self-assessment tool for use by transportation asset owners and operators. Currently, a maritime module is operational. Development efforts are underway for a General Aviation module and a Mass Transit module. TSA has also developed a tool in support of on-site, TSA-led vulnerability assessments. TSA intends to conduct on-site assessments of certain assets deemed to be nationally critical. Assessments have been completed for the Staten Island Ferry, the Port Authority of New York and New Jersey Bus Terminal, and the Woodrow Wilson Bridge construction project. Efforts are also underway in support of congressionally-mandated joint TSA/FBI assessments of critical airports.

13. Since its inception, TSA has focused on passenger aviation security, and in particular on passenger and baggage screening. Its budget has been heavily weighted toward the costs

associated with initiating and maintaining the aviation screening operation and has contained relatively little funding for other transportation modes. This pattern has continued in the agency's FY 2005 budget request.

a. Do you believe TSA needs to broaden its focus and undertake more efforts to improve security in areas outside passenger aviation screening?

Answer: TSA has been spending the majority of its funding and effort as directed by Congress towards what has been the largest and most consistent potential threat, attacks on our aviation system. At the same time, TSA has been working to improve security in other modes of transportation, including building cooperative relationships with our Federal, state, local and tribal government partners and our private sector partners. As part of the Department's risk management approach, TSA takes a broad view across transportation to identify security gaps and work with its partners to fill those gaps. Additionally, we are developing Sector Specific Protection Plan for the Transportation in accordance with Homeland Security Presidential Directive 7. I have discussed this effort in greater detail in other responses.

b. If so, what actions will you take and what resources will TSA need to accomplish these objectives?

Answer: The TSA vulnerability assessment methodology is based upon a wide array of potential threat scenarios. As an example, in the aviation sector, scenarios include aggressor paths beyond the passenger screening checkpoint. Scenarios include access through an airport perimeter, access through cross-perimeter buildings, and insider scenarios. The relative risk associated with these scenarios is being used as input into prioritizing investments in areas beyond aviation passenger screening. As discussed in many responses, partnership with transportation stakeholders is critical to accomplishing our collective objective to identify and address security gaps.

c. What is your timetable for undertaking these efforts?

Answer: Specific to aviation security assessments, TSA and FBI jointly updated the Joint FBI/TSA Vulnerability Assessment (JVA) tool and have commenced using it at commercial airports located in the vicinity of the G8 Conference, the Democratic National Convention and the Republican National Convention. In the fall, TSA will roll out the JVAs at all commercial airports. Data gathered during the JVA process will then be incorporated into a vulnerability self-assessment module for commercial airport. The commercial airport vulnerability self-assessment module will be instituted in 2005. Data collected from both tools will be analyzed, focusing on security gaps in areas outside of passenger security.

CAPPS II

14. One of the most sensitive and controversial programs being developed by TSA is the Computer Assisted Passenger Prescreening System (CAPPS II). The system is intended

to help in passenger screening; however, as recently reported by GAO, the system is behind schedule, how it will function is not fully known, key questions regarding the system's development and operation have not been answered, and other challenges such as identity theft and international cooperation have impeded system development.

a. When do you anticipate that CAPPS II will begin operation? When will the system be "certified" by the Under Secretary for Transportation and Border Security as required by P.L. 108-176?

Answer: CAPPS II is a fully integrated, basic functioning system that has been tested using simulated PNR data. Ultimately, the timeline for implementation of CAPPS II, and certification by the Under Secretary under the Vision 100 Act, is subject to receipt of PNR data for testing. To date, TSA has not secured PNR data to test CAPPS II. There are a number of formal steps that we must go through before we are in a position to receive PNR data. We are also currently developing our security program to ensure the integrity of the data once it is collected. Until we are confident that both the security system and redress procedures meet privacy and security muster, we have no intention of collecting PNR data for any reason.

Seven of the eight areas identified by the Congress in the Department of Homeland Security Appropriations Act, 2004 could not be satisfactorily reported by the GAO as having been completed, as they are contingent on testing of CAPPS II. However, TSA is well on its way to putting plans in place to meet each of the certification requirements including the establishment of redress procedures, the adoption of robust privacy protections, and the implementation of safeguards against abuse or unauthorized access.

b. A key challenge has been the inability to obtain passenger data from air carriers for testing purposes due to privacy concerns. We understand that TSA is planning on issuing a regulation to require that this data be provided. What considerations were given to addressing air carrier reluctance to provide passenger data? Why weren't actions initiated earlier to require the submission of data and thereby remove the concerns over privacy from air carriers?

Answer: TSA plans to use the Notice of Proposed Rulemaking (NPRM) vehicle to seek public comment on the collection of Passenger Name Record (PNR) data for the operation of the CAPPS II program, and would likely issue an order compelling the collection of historical PNR data for testing purposes simultaneously with publication of that NPRM. Each of these documents would require regulated parties to take reasonable steps to ensure that passengers are provided notice of the purpose for which the information is collected, the authority under which it is collected, and any consequences associated with a passenger's failure to provide the information.

However, system testing can only begin once TSA obtains a significant quantity of PNR data from airlines or from U.S. Customs and Border Protection (CBP) under the terms of an agreement DHS reached with the European Commission for CBP's use of such data, which has yet to be finalized.

Throughout the development process, privacy has been a foremost concern of TSA. The agency has made significant overtures to the general public and to specific stakeholder groups concerned about privacy issues, and supports the seven Passenger Privacy Principles recently released by the Air Transport Association (ATA), which are consistent with the Fair Information Principles used to develop the privacy management program for CAPPS II and the building block for the agency's privacy policies and practices.

The Privacy issues associated with the collection of data for testing are not a matter of timing, but one of disclosure. Simply stated, TSA's intention is to build public trust in the agency's ability to secure travelers' data – even test data – appropriately, and treat travelers fairly. To that end, now that the agreement reached with the European Commission on behalf of CBP, which permits TSA to test the CAPPS II system using EU PNR information, the agency anticipates being able to resolve within a few weeks when and how it will proceed with testing of the system, including the means by which the collection of data will be compelled.

c. A recent GAO report mentioned that identity theft could be used by individuals to defeat CAPPS II. What is TSA doing to ensure that potential terrorists could not negate the system's benefits through identity theft? Do you have any efforts underway to address this weakness?

Answer: While no system can be 100% effective in preventing identity theft, we believe that the CAPPS II system under development would represent a quantum leap forward in efforts to defeat this growing problem. TSA has developed CAPPS II to rely on an improved version of the best practices used by the banking and credit industries to combat identity theft and fraud.

Where a legitimate identity is stolen, there are any number of indicia, including errors or inconsistencies in the information as transmitted by a thief that could reveal that the identity is stolen. Further, CAPPS II will make use of a database containing up-to-date information about stolen identities, which will further protect against terrorists who use this means to conceal themselves.

Again, no system can be 100% effective, which is why CAPPS II will be part of a layered "system of systems" involving physical scrutiny, identity-based risk assessment, and other security precautions on aircraft and at airports.

d. International acceptance and cooperation on this system will be critical and although it has been noted that the European Union agreed to allow data related to its citizens to be used for testing purposes, there are still considerable concerns that the EU may not agree with the use of the currently proposed CAPPS II system to prescreen its citizens. What is your perspective on this issue? Do you believe full international cooperation will be attained, and why? In developing CAPPS II, has TSA attempted

to involve other countries in the system's development in order to obtain greater acceptance and use of the system?

Answer: As part of the PNR details of the agreement to be signed in the coming weeks, the European Commission pledged to enter into negotiations to find a legal framework for the transfer of PNR for use by CAPPS II. Under the framework of the agreement the EU, it is paramount that testing not be done with foreign data before it is done with US data. This will allow TSA to demonstrate to our foreign partners and to the domestic public that appropriate privacy safeguards are in place and that effective redress processes have been established.

TSA believes full international cooperation will be achieved. Passenger pre-screening is mandated by law and TSA, as part of DHS, remains committed to moving forward with the development and implementation of a better system than the CAPPS I system currently run by the airlines. TSA has been contacted by a number of other countries interested in our on-going work in this area. Having some of the most stringent privacy laws in place, negotiations with the EU offer the best opportunity to develop standards, which should be agreeable with all our international travel partners.

15. The President's budget requests $60 million for CAPPS II. How confident are you that $60 million will be sufficient and why? How much will be required for development, testing, and other one-time startup costs? How much in recurring costs will be required to maintain and operate the system on an annual basis?

Answer: The President's budget request at $60M will provide CAPPS II with continued facilities leases, utilities and maintenance, IT and telecommunications support, Infrastructure support (security, FTEs, etc), and System Development and operations. Systems Development and Operations includes: Contractor staff support for policy and privacy issue resolution, development of production platform to full capability, establishment of necessary connectivity to test PNR data live with a single airline, and capability of production platform to host other applications.

Facilities leases, Utilities and Maintenance	$ 3.3M
IT and Telecommunication	$ 5.2M
Infrastructure support (security, FTEs, etc.)	$10.8M
CAPPS II Development and Operations	$40.7M

Of the $60M in FY05, approximately $36M will be for development, testing, and other one-time start-up costs. The remaining $24M will be recurring costs, which include facilities leases, utilities and maintenance, IT and telecommunications support, and infrastructure support (security, FTEs, etc).

16. According to press reports, American Airlines authorized its vendor, Airline Automation, to provide TSA with one week's worth of Passenger Name Record ("PNR") data on its customers. The vendor then reportedly provided the data to four companies competing

for contracts with TSA: HNC Software, Infoglide Software, Ascent Technology, and Lockheed Martin.

a. Did any TSA official ask American Airlines or its vendor to provide PNR data to the agency or to any of the four companies? If so, why?

Answer: In early 2002, the Transportation Security Administration (TSA), at the direction of the Deputy Secretary of Transportation, started to work with the DOT's Office of the Chief Information Officer to begin examining the feasibility of a successor system to the Computer Assisted Passenger Prescreening System (CAPPS). CAPPS was previously developed by Federal Aviation Administration (FAA) and currently is operated by the domestic airlines. The successor system, known as CAPPS II, was contemplated as a risk assessment system that ultimately would be owned and operated by the government. As a precursor to building such a system, TSA decided to enlist the assistance of private sector firms with risk assessment expertise in a proof of concept exercise. The purpose of this exercise was not to develop an operation-ready system for purchase by TSA, but to prove the feasibility of the concept of performing a risk assessment, based on airline reservation information.

On March 8, 2002, the FAA, on behalf of TSA, issued a Broad Agency Announcement (BAA) soliciting proposals for the development of a Risk Assessment Engine (RAE) prototype that would be capable of assigning risk to such areas as passengers, flights, airlines, and airports across the nation. Among the eligibility criteria specified in the BAA was the requirement that companies demonstrate their ability to link with airline computer reservation systems and extract passenger name records (PNR) for risk assessment.

In anticipation of awarding cooperative agreements to qualified firms, TSA took steps to ensure that the cooperative agreement recipients would have a single set of PNRs to work with in demonstrating the feasibility of the RAE concept. To that end, TSA began discussions with Airline Automation, Inc. (AAI), which managed PNRs for a number of large domestic airlines, including American Airlines (American) and Continental Airlines (Continental).

On May 8, 2002, TSA and FAA entered into cooperative agreements with HNC Software, Infoglide, Ascent Technology, and Lockheed Martin (the cooperative agreement recipients) to develop RAE prototypes. TSA planned to evaluate the prototypes as candidates for further use as a component of CAPPS II. During the course of the performance of the cooperative agreements, some of the recipients told TSA they had difficulty in obtaining access to PNRs in order to demonstrate the capabilities of their prototypes to interface with airline reservation systems. This provided further impetus for TSA to arrange for the cooperative agreement recipients to have access to a single set of PNRs for purposes of the proof of concept.

To achieve this goal, TSA contacted American on May 20, 2002, and Continental, on May 22, 2002, to request that they each authorize AAI to provide PNRs to the

cooperative agreement recipients for purposes of developing the RAE prototypes. American authorized AAI to provide PNRs for this purpose, but Continental did not. AAI, therefore, did not provide PNRs from Continental. AAI provided American PNRs to the cooperative agreement recipients on March 24, 2002, in a format that was not usable. AAI subsequently made American PNRs available to the cooperative agreement recipients and to TSA by loading them on a secure server in June of 2002. The cooperative agreement recipients used the PNRs in order to perform the RAE proof of concept. TSA never accessed the PNRs on the secure server. However, during the demonstrations of the RAE prototypes put on by each cooperative agreement recipient, TSA officials viewed presentations that included PNR data as part of the demonstrations. Confidentiality of PNRs was protected under non-disclosure agreements entered into by the various parties. I understand that PNRs used in connection with performance of the cooperative agreements have been returned, destroyed or otherwise secured.

During the course of performance of the cooperative agreements, some of the cooperative agreement recipients independently obtained PNRs other than the American PNRs supplied by AAI. The independent sources of PNRs that TSA is specifically aware of are: Delta Air Lines (through Delta's Airline Reservation System); Continental, America West Airlines, and Frontier Airlines (through EDS/Shares); JetBlue (through Acxiom); Galileo International; and possibly Apollo; TSA did not have access to these PNRs.

b. How did TSA and/or the companies use the data? Was it for a CAPPS II-related purpose?

Answer: In the initial stages of examining the feasibility of developing a successor to CAPPS, TSA decided to enlist the assistance of private sector firms with risk assessment expertise in a proof of concept exercise. The purpose of this exercise was to prove the feasibility of performing a risk assessment for passengers, based on airline reservation information. Ultimately, the successful demonstration of such a process could lead to the development of a commercial product that would become part of CAPPS II. Although TSA had access to PNRs that AAI placed on a secure server, TSA never actually accessed them, and therefore, did not use PNRs for any purpose. However, during the demonstrations of the RAE prototypes put on by each cooperative agreement recipient, TSA officials viewed presentations that included PNR data as part of the demonstrations. The cooperative agreement recipients used PNRs to develop their RAE prototypes in furtherance of their cooperative agreements with TSA.

c. Which, if any, of the four companies possessed PNR data while performing contract work for TSA? If so, was the work related to CAPPS II?

Answer: For purposes of developing a risk assessment prototype, the four companies were working with TSA pursuant to cooperative agreements, not contracts. The purpose of TSA's relationship with these four companies was not to contract for the procurement an operation-ready system. As a precursor to any government contracting effort, TSA sought to research the feasibility of performing a risk assessment for passengers using airline reservation information as the basis for the assessment. Ultimately, the successful

demonstration of such a process could lead to the development of a commercial product that would become part of CAPPS II. In the course of performing under the cooperative agreements, all four cooperative agreement recipients possessed PNR data.

d. Did TSA or any of the companies create a system of records as defined by the Privacy Act (5 U.S.C. 552a(a))? If not, please explain how the collection and use of the information does not meet the Act's definition of a system of records.

Answer: My understanding is that at the time that TSA was involved in ensuring that cooperative agreement recipients had access to passenger name data (PNRs), which was prior to the existence of DHS, personnel at TSA evaluated the matter and believed that their actions were fully in compliance with the Privacy Act. No System of Records Notice was written. TSA facilitated the transfer of the PNR data to be used as a data set, rather than to be retrieved by name or personal identifier. The data set was to be used for the purpose of testing the functionality of a "Risk Assessment Engine Prototype" for identity-based security threat assessment technologies. Since the information was not to be accessed or retrieved by name or personal identifier to make individual determinations, TSA believed that it did not need to publish a system of records notice under the Privacy Act. Additionally, they believed that even if testing constituted a Privacy Act system, it could be covered by a pre-existing system of records applicable to the program.

I appreciate that since the time of TSA's assessment, further questions have been raised about these PNR transfers. Also since that time, DHS was established by Congress and TSA, formerly under the Department of Transportation, became a component agency of DHS. As you may know, the Chief Privacy Officer at the Department of Homeland Security has initiated a comprehensive examination of the circumstances surrounding TSA's involvement in the data sharing from airlines that took place before TSA's integration into DHS. I fully endorse this examination for the lessons that can be learned and I am assisting in every way possible. Based on that review, I commit to you that I will use my leadership role to expeditiously take appropriate steps as warranted. On that note, let me further assure you that as Acting TSA Administrator, with the fullest support from Secretary Ridge, Deputy Secretary Loy, and Under Secretary Hutchinson, I tasked a senior level TSA team to begin intensive efforts for TSA-wide privacy training. I have also hired a TSA Privacy Officer to assist with all TSA privacy related policy and program reviews, in collaboration with the DHS Chief Privacy Officer. All of these initiatives have been accomplished, with full participation by TSA staff. I have the highest confidence in my senior management and staff, and I commend their ongoing positive reception of privacy compliance and sensitivity as integral to carrying out TSA's part in the Department of Homeland Security mission. It is one of many reasons why, if confirmed, I look forward to leading the TSA team within the Department of Homeland Security.

e. TSA has requested PNR data from JetBlue (on behalf of an Army contractor) and from American Airlines. Has TSA requested that any other airlines provide PNR data?

Answer: As discussed below, TSA requested PNR data from three other companies unconnected to specific investigations: Continental Airlines, Delta Air Lines, and Sabre. In addition, in the spring of 2003, TSA obtained PNRs from JetBlue in order to determine whether changes could be made to the CAPPS system that would address what appeared to be a disproportionate impact of that system on passengers of certain airlines. TSA used the information contained in the PNRs supplied by JetBlue to test the application of a modified risk assessment algorithm for CAPPS. The PNR data was not provided to any other party. TSA has retained the PNRs because of a pending FOIA request that is broad enough to encompass this data.

On May 22, 2002, TSA requested PNRs from Continental Airlines for use by the cooperative agreement recipients in developing RAE prototypes. Although TSA and Continental executed a non-disclosure agreement in contemplation of Continental providing PNRs for this purposes, Continental ultimately did not provide any PNRs.
In February 2002, TSA directed Delta Air Lines to provide PNRs to the U.S. Secret Service in connection with security preparations for the Salt Lake City Winter Olympics, which was a National Special Security Event. The U.S. Secret Service used the PNRs (transmitted through ARINC) to alert the agency to the travel plans of individuals of known protective interest. The records were stored in a stand-alone computer located at the Intelligence Division Duty Desk. Although a non-disclosure agreement signed by Delta Air Lines and USSS stated that PNRs might be disseminated to InRange Technologies Corporation, PNRs were not shared with any parties outside the U.S. Secret Service and were disposed of after the event.

In February 2003, TSA requested PNRs from Delta Air Lines for use by IBM Global Services, which was under contract to TSA to develop an airline data interface that would serve as the conduit through which PNR data would flow between the CAPPS II risk assessment engine and the airlines. On February 27, 2003, Delta transmitted an unknown number of what TSA and IBM thought were actual PNRs, but that Delta has since advised were artificial PNRs created by Delta engineers. On March 3, 2003, Delta requested that the data be deleted, and that request was honored that same day.
In May of 2003, TSA received a computer disk containing an unknown number of PNRs from Sabre in contemplation of using them to test existing components of the CAPPS II system. TSA returned the disk in September of 2003. While the disk was in TSA's possession, no one read the PNRs or otherwise attempted to obtain access to any information on the computer disk.

f. How does TSA plan to obtain PNR data to test CAPPS II? Is it considering promulgating new rules or issuing a security directive?

Answer: TSA plans to use the Notice of Proposed Rulemaking (NPRM) vehicle to seek public comment on the collection of Passenger Name Record (PNR) data for the operation of the CAPPS II program, and would likely issue an order compelling the collection of historical PNR data for testing purposes simultaneously with publication of that NPRM. Each of these documents would require regulated parties to take reasonable

steps to ensure that passengers are provided notice of the purpose for which the information is collected, the authority under which it is collected, and any consequences associated with a passenger's failure to provide the information.

g. When will CAPPS II testing begin and what safeguards could you put in place to ensure that the PNR data collected for testing purposes will be handled in a way that protects the privacy of airline passengers?

Answer: TSA is currently working with a number of contractors, privacy advocates and other stakeholders as well as meeting internally to discuss the data security and integrity aspects of CAPPS II. We are ensuring a very deliberative process to make certain that both the Information Technology as well as the Policy components are well-planned before any testing of the system is considered.

Currently, only TSA personnel and entities holding Top Secret level clearances and have a strict "need to know" will be considered for access to the CAPPS II system. All personnel and/or entities requiring access to the system will be vetted by the TSA and a risk assessment will be conducted on all individuals intending to connect to the system. Further, all entities will be subject to a Memorandum of Understanding (MOU) outlining roles, responsibilities, rules of behavior and consequences resulting from non-compliance with the MOU with respect to access to the system. To ensure compliance with the MOU and other agreements, extensive oversight, monitoring, and auditing of the system will be conducted by the Office of National Risk Assessment (ONRA) Information Systems Security to ensure compliance with established system rules of behavior.

The Information Systems Security Officer (ISSO) will preside over all the auditing and information systems, ensuring compliance with the above-mentioned standards of protection. In addition the ISSO will provide for the protection of information systems against unauthorized access and ensure that safeguards are implemented for the protection of the integrity, availability, and confidentiality of Information Technology resources.

One of the auditing safeguards that TSA will rely upon for CAPPS II is software called Radiant Trust™. Radiant Trust™ maintains audit trails of who accessed the system and the time/date as well as keeping records of all system activity. Working with other security programs, Radiant Trust™ will detect any security violation, performance problems and flaws in applications. Furthermore, the system access controls on Radiant Trust will be strict. A two-person approval process will be necessary to ensure that access is given to authorized personnel only.

CAPPS II testing will not begin until security systems to ensure protection of the data are fully in place.

h. Do you agree with the steps TSA has taken thus far to secure PNR data to develop or test CAPPS II?

Answer: To date, TSA has not secured PNR data to test CAPPS II. As noted in my responses to Question 11 above, there are a number of formal steps that we must go through before we are in a position to receive PNR data. We are also currently developing our security program to ensure the integrity of the data once it is collected. Until we are confident that both the security system and redress procedures meet privacy and security muster, we have no intention of collecting PNR data for any reason.

17. According to a TSA fact sheet released September 29, 2003, "CAPPS II will authenticate the identity of passengers by checking the passenger name record - including full name, home address, telephone number and date of birth - against commercial databases. In addition, a risk assessment will be done by checking passenger names against government databases." During the consideration of his nomination, Admiral Loy was asked how difficult it would be for a terrorist to acquire over the Internet or through other means the four personal data elements (name, home address, telephone number and date of birth) of law-abiding Americans who are not likely to be assigned yellow or red ratings by the CAPPS II system. He responded that "with CAPPS II, the four PNR data elements start a process of authentication, which validates and verifies information provided by the individual. With only these four data items, a terrorist would not necessarily receive a high enough authentication and risk assessment score to be assigned a green rating by the CAPPS II system."

If a terrorist successfully acquired the four personal data elements of an American not likely to be assigned yellow or red ratings by the CAPPS II system, and if that PNR data is all that is provided to commercial databases, how will the process of authentication used by commercial databases discern that the passenger is not who he purports to be?

Answer: In cases where an individual attempts to travel using a reported stolen or fraudulent identity, the identity authentication function of CAPPS II can detect it, through the use of both government and public source databases. Commercial information providers that currently provide the same service to other commercial entities in the fields of banking, insurance, and credit will conduct the CAPPS II identity authentication. The authentication process used by CAPPS II will rely on more than just the four personal data elements. Accordingly, merely obtaining those elements would not be sufficient to defeat the system. Further, if the identity theft has been reported, that information would be available in commercial databases. It is also important to note that CAPPS II is part of a system of systems that includes screening of passengers and their checked and carry-on baggage, the display of valid, government-issued photo identification, Federal Air Marshals, Federal Flight Deck Officers, hardened cockpit doors, and other enhanced security practices. Each security measure is designed to complement the efficiency and effectiveness of the others. The result is a system of enhanced security systems designed to provide a layered security that addresses a continuum of security threats with minimal impact on airline customers and operations, and on the free flow of commerce through the nation's commercial aviation infrastructure.

18. The CAPPS II system appears likely to assign yellow ratings to large numbers of travelers for reasons unrelated to any threat they may pose. The authentication process

used by commercial databases seems likely to select for people who have changed their addresses frequently, suggesting that college students, members of the Armed Forces, and people who move often for job-related reasons will more likely be assigned yellow ratings. The system may also select for extra scrutiny people who have recently changed their names, such as recently married women, and people who do not have substantial credit and billing histories.

a. Do you agree that these groups are more likely to be assigned yellow ratings? Please explain.

Answer: No. The CAPPS II identity authentication procedure as currently designed will take information provided by a given individual and attempt to confirm that individual's identity by finding consistent, publicly available information about that individual in commercial databases. CAPPS II uses a number of public commercial databases to confirm an identity. A simple address change or name change would not elevate an individual's risk score, since these occur frequently and are generally quickly reflected in various databases which will be used to support CAPPS II.

b. If individuals are frequently searched more extensively for reasons unrelated to security, what remedies, if any, will they have to seek modifications to the way they are graded by the CAPPS II system?

Answer: Procedures are being designed that will address the complaints from passengers who believe the system has incorrectly or consistently identified them for additional screening. An essential part of the redress process is the establishment of the CAPPS II Passenger Advocate. The Passenger Advocate will focus on assisting passengers who feel that they have been incorrectly or consistently prescreened.

TSA is also working with commercial data aggregators to establish appropriate procedures to allow the passenger to contact the commercial data providers to determine, update, and correct information that may be inconsistent.[1] TSA will create procedures by which the Government may identify and correct inconsistent data derived from law enforcement data systems. TSA's procedures will also specifically address ways to identify and reduce the additional screening that results when one passenger coincidentally has a name and other personal information that may closely approximate similar data on a person of special interest to the Government (and who may therefore be on watchlist). As stated earlier, however, the use of best industry practices in identification verification technology is expected to greatly limit these occurrences.

19. The TSA's most recent Privacy Act Notice for CAPPS II disclosed that CAPPS II will be linked with the U.S. VISIT program. Why will CAPPS II be linked with the U.S. VISIT program? Will CAPPS II be used to identify out of status foreign nationals in the absence of any evidence that they pose a risk to commercial aviation?

[1] Inconsistent data may not directly reflect on the accuracy, completeness or timeliness of the data. Rather, it is a term used to describe conditions in which one data set conflicts with another data set (e.g. a person provides an older home address rather than the most current home address).

Answer: As indicated in the interim Privacy Act notice published last August, CAPPS II is designed to identify known and potential terrorists or their associates, or those who are subject to outstanding warrants for certain crimes of violence. TSA remains committed to maintaining a narrow focus on the appropriate uses of CAPPS II. Prior to implementation of the program, TSA will publish a rule-making and a privacy policy, which will clearly set forth the parameters of the program. There have been no discussions to modify the NPRM in order to use CAPPS II for visa violators. Furthermore, although the Privacy Act referenced potential connectivity between CAPPS II and US-VISIT, there are no current plans to merge the CAPPS II and US-VISIT programs. They not only have significant differences in terms of mission and scope, but also how data are used, stored, and retained. The two systems are being kept separate and distinct, but we do recognize that there may be opportunities, in the future, for the two systems to communicate with each other. The purpose of this communication would be to ensure that both programs leverage the most accurate and current data to prevent the entry of terrorists and criminals and to prevent the misidentification of innocent travelers. As part of any future plan to share the information from the two programs, DHS would ensure privacy-enhancing safeguards were taken and impose strict rules about which agencies could use the passenger information and for what specific purposes.

20. According to news reports, ChoicePoint, a leading commercial database company, recently opted out of participation in the CAPPS II program because of a disagreement with TSA's approach. This month, the company's CEO said the TSA should be pursuing a "link analysis" approach rather than its current strategy, which he reportedly compared to the Total Information Awareness program once proposed by the Department of Defense. What is your response to that analysis?

Answer: This analysis is inaccurate and does not reflect TSA's strategy. First, ChoicePoint was never awarded any contract or subcontract under the CAPPS II program, so reports that they have "opted out of participation" are misleading.

Moreover, based on these reported statements, they are apparently unfamiliar with TSA's current strategy. TSA is pursuing many techniques, including "link analysis." On the other hand, comparisons to the Total Information Awareness (TIA) program are unfounded because CAPPS II has never included the profiling and the extensive use of personal information that TIA proposed in order to determine patterns of behavior and associations.. In fact, CAPPS II was designed to never allow commercial data within the Government firewall, ensuring a major privacy safeguard. The only information passed through the CAPPS II firewall from commercial data aggregators will be a generic score indicating confidence in the passenger's identity. Thus, with all due respect to ChoicePoint's CEO, I disagree with his statement.

PASSENGER SCREENING

21. GAO and the DHS OIG recently reported that screeners are performing poorly in detecting threat objects. What steps should be taken to improve screener performance?

Answer: I believe it should be recognized that both reports also indicated that TSA has made significant progress of late to provide enhanced training products to the screener workforce to improve threat object detection performance. And, we have already taken significant steps we believe will enhance screener performance.

Since January 2004 TSA has implemented a number of initiatives to improve screener performance with respect to detecting threat objects, and we are seeing a steady increase in screener performance as indicated by covert testing conducted by our Office of Internal Affairs and Program Review. These efforts include:

- Full implementation of the Threat Image Projection (TIP) system: TIP superimposes randomly selected threat images on x-ray screens during actual operations and records whether or not screeners identify the threat object. This embedded training and performance monitoring tool provides results from each TIP Ready X-ray (TRX) machine allowing supervisors and FSDs to monitor individual screener so that a training plan can be developed with a direct focus on areas needing improvement. Concurrent with the reactivation and expansion of the TIP program to all checkpoints, we implemented a significantly expanded library of 2400 images categorized by difficulty.

- Distribution of Modular Bomb Sets (MBS II) and inert weapons training kits: All airports received at least one set of kits with larger airports getting up to three sets. These kits permit screeners to be directly familiar with improvised explosive device (IED) components and weapons and to determine how they would appear on an x-ray image both completely assembled and in partial configuration. Guidance on the use of these kits by FSDs for local covert operational testing was provided to the field and local testing is on going.

- Delivery of new "X-Ray Tutor" image interpretation course: X-Ray Tutor is a computer based training course available to screeners to practice interpreting x-ray images and identifying threat objects. Similar to TIP, the system records correct and incorrect interpretation results and provides direct feedback to the screener when an object is missed. The use of the "X-Ray Tutor" program is recommended for an average of 1-hour per week by each screener as part of their 3-hours of weekly recurrent training.

- Introduction of a "Threat in the Spot Light" program: This program consists of a weekly series of articles written specifically for Screeners and Screener Supervisors that describe and show actual pictures, and in some cases, x-ray presentations, of threats found by screeners at airports or from other operational/intelligence resources.

- Development of videos and interactive web/computer based training courses titled "Excellence in Screener Performance": This training is intended to support the

requirement for FSDs to provide a minimum of 3-hours of recurrent training per week averaged over the month. Topics include:

- Handwanding and Pat-down
- Customer Service
- Checkpoint and Checked Baggage Operations
- Physical Bag Search
- EDS Operations
- X-ray Operator

Additional videos and web/computer-based training are in the design/development stage and will be released during the summer and fall.

22. At an April 22, 2004 hearing before the House Aviation Subcommittee, GAO, the DHS OIG, and BearingPoint (the consultant that did an evaluation of the private contractor screening pilot program) stated that TSA has yet to establish performance standards to measure the performance of screeners. Is this the case? If so, when will TSA establish such standards?

Answer: TSA established initial performance standards for all screeners as part of the Performance Management System in FY 2002. In addition, TSA is finishing an analysis of initial Threat Image Projection (TIP) system performance data and setting National performance standards for all screeners. Interim performance standards for TIP were disseminated to all Federal Security Directors in March 2004, and the final standards are expected during the Summer 2004. In addition, TSA implemented proficiency standards for screeners to meet during their assessments and evaluations that take place at the completion of their Basic Screener Training, On-The-Job Screener Training (i.e., initial Certification), and annual Re-certification. In addition to passing three modules of assessments, screeners have always had to achieve a "meets or exceeds standards" on their annual performance rating as part of their re-certification requirement.

23. Last year, TSA was forced to reprogram most of its research and development **(**R&D**)** funding to cover personnel costs, largely associated with the screener workforce. R&D is key to improving aviation security and passenger screening. Have you or are you planning to reprogram any of this year's fiscal year's appropriation for R&D? What progress are you making in developing technologies to improve aviation security?

Answer: We have no plans to reprogram any of the FY 2004 R&D funding. Below is a representative sample of the progress TSA is making in developing technologies to improve aviation security in its four R&D program areas of Passenger, Commerce, Conveyance, and Infrastructure. These efforts are being funded through TSA's FY 2004 R&D budget and have been fully coordinated with the Department's Science and Technology directorate.

Passenger

- **Explosives Detection Portals** – operational testing and evaluation in the 3rd quarter

of FY 04. TSA has selected 5 airports for the pilot testing and the first pilot will begin June 14 at Providence, Rhode Island.

- **Document Scanners** – technical evaluations are underway using a manual technology that requires screener interaction, and while that is underway to determine operational suitability TSA is working to develop an automated technology that will not require screener interaction.
- **Explosives detection systems (EDS) for carry-on baggage.** TSA is planning to pilot a small unit that is currently in the lab for certification as an EDS at a checkpoint in the 4th quarter of FY 04. This automated system will look for explosive in carry-on baggage. In addition we have a robust R&D project ongoing that is looking for equipment that will not only automate the search for explosives in carry-on baggage but weapons as well. The prototype of this type of technology is approximately 1-2 year's away from operational testing.

Commerce (to include checked baggage and cargo)

- **Checked Baggage:** Next Generation EDS: Research and development to increase throughput, improve detection capabilities and lower alarm rates deliverables from vendors expected in the 4th quarter FY 2004 and 1st quarter FY 2005
- **Checked Baggage - Threat Image Projection (TIP) system:** Request for Proposals (RFP) has been issued to develop TIP capabilities for EDS systems to expose screeners to current threats and measure performance
- **Checked Baggage:** Training is underway to implement on-screen alarm resolution for EDS systems
- **Cargo:** Issued a market survey in January 2004, soliciting submissions and participation of vendors of commercial off-the-shelf explosives detection technology to support cargo inspection. Technologies have been selected for laboratory evaluation and operational testing and evaluation at 5 airports to begin in 3rd quarter and end in the 4th quarter of FY 2004.
- **Cargo:** Issued a RFP for potential developers of promising technologies in the area of explosives detection technology for cargo screening. The RFP was issued in February 2004, proposals have been evaluated and 15 of the 74 potential technology solutions have been selected for further consideration. TSA anticipates awarding R&D grants in the 4th quarter of FY 2004.
- **Cargo:** Continued support of TSA and CBP pilot of pulsed fast neutron analysis (PFNA) technology pilot to support containerized cargo screening.

Conveyance

- **Explosives Equivalency Assessments:** R&D efforts underway to determine the equivalent amount of explosives which would be necessary to cause catastrophic damage to trains, vessels, etc. compared to the documented amounts applicable to aircraft. Defining catastrophic levels will assist in the development of countermeasures and mitigation technology. Pilot testing of technologies underway at one rail station.

- **Aircraft:** Continue R&D efforts to design blast resistant cabin and cargo liners, as well as overhead bin mitigation technological solutions. TSA is also partnering with FAA and aircraft manufacturers to determine which solutions might be candidates for retrofitting, versus incorporation into initial aircraft designs.
- **Aircraft:** Continue susceptibility assessments for MANPADS and standoff weapons.

Infrastructure

- **20 Airport Access Control Pilot Program -** Initiated 8 of 10 pilot projects in 3rd quarter of FY 2004, preparing technology plans for remaining 2 airports to be included in Phase I implementation. TSA will complete 10 pilot program projects by the end of CY 2004.
- **$17 million Airport Terminal Security Improvement Grants** - TSA has issued 19 grants to airports to support terminal security improvement projects.
- **Biometrics Standards Development** - continue R&D efforts to establish standards for biometric systems through ongoing pilot programs and laboratory efforts.

24. On May 14, 2004, TSA released its plan for reallocating screeners among commercial airports under the 45,000 full-time equivalent screener cap.

a. When will TSA complete all the changes anticipated under this plan, including hiring new screeners at airports that are slated to receive additional screeners?

Answer: TSA has begun the process to incorporate the changes established with the latest allocation of screeners. We are currently underway for hiring at those airports that require more screeners and are prioritizing the high volume / high risk airports. TSA expects to have these screeners on board by July.

b. Have you received any objections to the reallocations? If so, how will you resolve those objections?

Answer: In the few cases where TSA has received requests to reassess reallocations, we have reviewed the factors leading to decisions made for those airports and explored the specific concerns or issues being raised. TSA has committed to assess staffing allocations through a periodic review to ensure that TSA is keeping pace with the dynamic nature of the aviation industry. In cases where further examination supports higher staffing levels, TSA will work to increase staffing at those airports within the statutory cap of 45,000 full-time equivalents screeners. Consequently, these increases can only occur if other airports lose an equal number of FTE screeners. TSA will have to prioritize its screener allocations based on the greatest need.

c. Based on the results of this plan, do you believe that the current cap on screeners should be increased or eliminated?

Answer: TSA reviews the workforce requirements for each airport on a periodic basis. As discussed in the response question #16, TSA has contracted with Regal to develop a "bottom-up" model designed to use airport-specific data to derive highly accurate staffing and throughput projections. This tool, once operational, will be an important asset in TSA's efforts to ensure that our screeners are deployed effectively to maximize the safety and security of the traveling public. This will also allow us to engage in further discussions with the relevant Committees of Congress.

TSA is also creating additional capacity through achieving greater efficiencies in the scheduling of screeners. Federal Security Directors at each airport now have access to scheduling tools that provide real-time information enabling them to forecast periods of peak demand for screening. TSA uses mores split shifts and has restructured the workforce to reach a higher ratio of part-time screeners to maximize operational flexibility. As a result of this restructuring, TSA can more efficiently schedule screeners to match capacity with the level of demand.

25. In your May 13, 2004 testimony before the House Subcommittee on Aviation, you outlined TSA's plans for handling the peak summer air travel season. You noted that Federal Security Directors (FSDs) "will be directed to ensure full screening capability, including use of overtime. This will include aggressive management of leave and vacation schedules, keeping checkpoints open longer on critical travel days…" Your testimony also states that FSDs will need to take steps to avert screener stress under this plan. If airports that warrant additional screeners under the reallocation plan are not fully staffed, how will FSDs ensure that existing screeners are not over-worked this summer and can operate at peak performance during a potentially difficult period?

Answer: TSA is working rapidly to bring airports on-board screener strength to their allocated numbers by July. At airports requiring additional work hours, FSDs will ensure screeners are scheduled very efficiently to minimize the amount of extra hours necessary. Additionally, overtime duties will be rotated among screeners as necessary to avoid unnecessary burdens.

26. During the April 22nd hearing before the Aviation Subcommittee, you stated that TSA would have a plan for the security screening opt out program by May 19, 2004. What criteria will you use to determine whether an airport can opt out?

Answer: TSA has forwarded its proposal to the Department and program guidance will be published soon, as promised, by early summer. As ATSA does not identify specific criteria for evaluation of the airport application, TSA is reviewing possible criteria and may consider factors such as the airport's record of compliance on security regulations and requirements, peak travel season needs, proximity to other airports opting out, cost factors, and TSA's hub and spoke airport configuration to determine the participation of airports in the Opt Out program, and the sequence of airports for transition from federal screeners to private screeners.

This program guidance will cover key issues, such as liability, funding, roles of the airport, the private screening contractor, the Federal Security Director and TSA headquarters — that will help airports gauge their interest.

27. Who within TSA will make the determination about whether to approve an airport's application to opt out?

Answer: TSA is developing the specific process for reviewing and approving airport applications. Whether or not I delegate any of this responsibility within TSA, as Acting Administrator I remain responsible for ensuring that the statutory requirements relating to the Opt Out program are carried out. As required by ATSA, TSA cannot enter into a contract with a private screening company under the Opt Out program unless the Administrator certifies to Congress that the private screening company is owned and controlled by a citizen of the United States, to the extent that the Administrator determines that there are private screening companies owned and controlled by such citizens.

28. Will federal screeners at airports that opt out be given first right of refusal for jobs with the private contractors?

Answer: TSA's goal is to transition from federal to private screening operations as efficiently and expeditiously as possible, maintaining security and minimizing any impact on customer service, while providing as considerate and well-managed a transition as possible for the affected workforce.

TSA will strive for a transition process that is fair, cost-effective and seamless. TSA believes that it is in everyone's best interest to leverage the current workforce, both from security (TSA has experienced screeners with training) and cost-effectiveness (assessing and training new screeners can entail significant costs) perspectives.

The program is still under development and further details have yet to be decided. However, TSA is supportive of provisions that assist current Federal screeners (screener, lead, and supervisors) potentially affected by the transition, to include a right of first refusal, and measures to facilitate movement to other TSA or other Federal positions. Under the Aviation and Transportation Security Act, the Federal Security Directors (FSD) are still responsible for security at the airport, including supervising screening at the airport, so the FSD and his or her staff would remain at the airports and would still be employees of the federal government.

29. Have you made any initial decisions about how the program will be structured and managed, e.g., establishing clearly delineated roles and authority for TSA headquarters, FSDs and their staff, airports and contractors?

Answer: The Opt Out program guidance TSA is drafting will clearly delineate the roles of the TSA headquarters, Federal Security Directors, airports, and contractors. I will be pleased to provide the Committee a copy of the guidance when it is available for release.

30. Under ATSA, airports can choose to "opt-out" of the federal screener program and utilize private screeners beginning in November 2004.

a. What effect will allowing airports to "opt-out" of the federal screener program have on TSA's ability to maintain uniform standards for passenger and baggage screening and ensure passenger safety?

Answer: TSA will continue to set one standard for security for the entire commercial aviation system, whether an airport has Federal screeners or private contractor screeners. TSA will ensure that standards are met by through TSA security protocols, extensive contract oversight, covert testing by TSA's Office of Internal Affairs and Program Review, and by continued oversight by Federal Security Directors (FSDs) and their staff in both federal and "opt out" airports.

Per ATSA, TSA is to supervise private screening services at each Opt Out airport. Private screeners must perform at the same or better level as Federal screeners and comply with Federal passenger and baggage screening standard operating procedures, as set forth in ATSA. ATSA also gives TSA the ability to terminate a contract with a private screening firm for repeatedly failing to perform.

b. What steps will you take to ensure that TSA's standards for screener hiring, training and proficiency are met by private screener operations?

Answer: Consistent with findings of the BearingPoint study, TSA is working out the optimal approach to provide more local flexibility in a manner that meets Federal security standards and is also cost effective. For example, TSA is currently reviewing hiring and training processes in both the PP5 and Federal airports and is conducting a pilot program in Boston to allow more local flexibility in hiring. Private contractor operations will need to meet the same screener qualification standards that TSA must meet with Federal screeners, per ATSA. TSA will continue to maintain security protocols and Standard Operating Procedures. TSA will take several steps to ensure that training and security standards are met including: contractual terms with the private companies, FSD oversight, annual recertification of screeners, quality assurance reviews, covert testing, and requirements for contractors to keep training records.

c. Do you believe airports should be encouraged to retain the TSA federal screener program? If so, what actions will you take to do so? If not, please explain.

Answer: ATSA states that TSA shall allow an airport operator to submit an application to have screening carried out by the screening personnel of a qualified private screening company. TSA is committed to developing a fair, balanced program that does the following (no ranking of importance implied by order):

- Meets ATSA standards
- Ensures security

- Seeks to establish a strong public / private partnership
- Provides significant opportunity for innovation, efficiency, and cost savings to the taxpayer
- Provides decentralized management
- Incorporates best practices and lessons learned from recent studies of the Pilot program, and continues to evaluate and learn on an on-going basis
- Is performance-based
- Does not restrict airport participation
- Respects federal and private sector workforces

Under ATSA, the decision to apply for private screening services lies with individual airport operators. However, should TSA approve the application, TSA will continue to oversee airport security, whether an airport has private contract screeners or federal screeners.

31. In accordance with the requirements of ATSA, TSA set up pilot projects at five commercial airports that were allowed to utilize privately contracted screening personnel. TSA commissioned a study from BearingPoint to compare the performance of the private screeners to the federal airport screeners employed by TSA; this report was released at a House Aviation Subcommittee hearing on April 22, 2004.

a. You testified at that hearing that federal screener performance had improved by 70% over the last 18 months, but the DHS Inspector General questioned whether that level of improvement had occurred. In fact, the IG testified that, although testing of private and federal screener performance showed comparable results, there has been little or no improvement in screener performance since the 9/11 attacks. Please explain the basis for your statement that federal screener performance has improved. Does the Inspector General have that information?

Answer: TSA began testing its screeners in September 2002. The 70 percent improvement is derived from comparing the overall checkpoint test results from this first period of testing to the more recent overall checkpoint test results for the period ending March 31, 2004. Thus, the 70 percent improvement is based on a comparison of these two points in time.

TSA conducts three basic types of checkpoint tests: weapon on person, weapon in a carry-on bag, and inert improvised explosive device (IED) in a carry-on bag. Since September 2002, TSA has increased the difficulty in several of these testing protocols and added additional tests to its covert testing program, including a test with an IED in a shoe. Even with these changes, the overall checkpoint test results have climbed steadily between September 2002 and March 31, 2004.

TSA uses covert test results as one indicator of screener performance. The covert testing program, which issues status reports to TSA officials, had disclosed vulnerabilities in screener performance that TSA had to address. Between October 1, 2003, and March 31, 2004, TSA implemented several specific training initiatives as part of the Screening

Performance Improvement Program. As part of this program, the Office of Internal Affairs and Program Review (OIAPR), which is responsible for TSA's covert testing program, agreed to continue conducting first time tests at airports and to retest airports once the training initiatives had been implemented. Between January 1, 2004, and March 31, 2004, OIAPR retested 44 airports and found that 32 airports had improved overall checkpoint test results.

Since TSA testified on April 22, 2004, OIAPR has met with representatives from the Office of Inspector General to discuss in detail its covert test results and to provide comprehensive data showing the basis for the 70 percent improvement as well as the overall improvement in checkpoint test results and test results by test object. In addition, OIAPR provided the Office of Inspector General copies of the relevant briefing documents that were shared with congressional staff and formed the basis of TSA's testimony on covert testing and screener performance.

b. BearingPoint's report noted several factors that it said impeded its ability to make a true comparison between the use of federal and private screeners, including the small number of airports in the pilot study, the limited amount of data available for review and analysis and the extent to which the private screening force was affected by federal decision-making. Do you agree with these concerns? Will this report be of use to you in designing TSA's process under which airports can apply to "opt out" of the federal screener program beginning in November or do you believe its utility is limited by the factors raised by BearingPoint? Please explain.

Answer: TSA recognized that the PP5 program created a valuable opportunity to learn about operational improvements that could be incorporated into the Screening Partnership Program (Opt Out). As a result, a key requirement of the Bearing Point evaluation of the PP5 program was to identify areas for improvement and make recommendations. TSA believes these ideas will be valuable in the development of the Screening Partnership Program (Opt Out). TSA is analyzing the recommendations and plans to incorporate several of them including:

a. Increase decentralization and local empowerment across airports, particularly in the areas of assessment and screener technical training;

b. Analyze performance measurement: work toward service level agreements and performance measures with more specific targets.

While Bearing Point noted some constraints in the study, such as the small number of airports studied, they concluded that they did not affect the overall utility of the study's conclusions.

32. GAO's testimony at the April 22 House Aviation Subcommittee hearing noted that both private screening contractors and Federal Security Directors (FSDs) overseeing TSA screeners faced challenges in achieving appropriate staffing levels and ensuring that

screener staff performed optimally due to the level of control TSA exercises from headquarters over airport screening operations. (GAO-04-505T)

a. As FSD for the Los Angeles airport, what was your experience in managing the airport's screening operations under TSA's centralized controls over screener hiring, training and other operational matters? Did TSA's exercise of control over such areas affect your ability to meet needed staffing levels, provide adequate training for screeners and otherwise perform expected security functions effectively? Please explain.

Answer: During my tenure as the Federal Security Director for Los Angeles International Airport (LAX), TSA was a fledgling Federal agency rolling out security screening programs at hundreds of airports and hiring, training, and deploying thousands of screeners across the country. Since that time, I have seen from my vantage point as Acting Administrator that TSA has matured into a fully realized Federal agency which is setting the mark for other Federal and non-Federal entities involved in transportation security. While TSA was in its start-up phase, centralization of hiring, training, and other operational matters made perfect sense. Meeting the milestones that Congress set for the agency would have been impossible if these processes were not centralized.

Now that we are into our third year, we have had the opportunity to review our organization and are making changes that make sense as we continue to mature as an agency. We have instituted local testing at our airports, so that the FSDs can challenge their screeners to continue to learn and grow. Our "train the trainer" program was introduced almost a year ago for cross-training our screeners for different screening functions, and is now in use for the initial training of screeners at their home airports. We are also in the process of allowing local screener hiring, so that FSDs will have more agility in addressing their hiring needs. I believe that these initiatives will allow our FSDs to have the flexibility they need to perform their security functions more effectively by giving them more direct authority. TSA will continue to hold FSDs accountable for meeting federal security standards, and for managing effectively. If confirmed I will continue these efforts to strike the right balance between effective agency-wide management and local FSD authority.

b. Do you plan to provide more flexibility to FSDs overseeing federal screeners and private screening contractors in hiring and other operational matters and, if so, what changes will you make? Should private screening contractors and airports with federal screeners receive the same flexibilities? If you provide additional flexibilities, what steps will you take to ensure consistency in screener operations across the nation's airports?

Answer: I am committed to providing more flexibility to FSDs at both federal and private screening airports. I want to include more local decision-making for hiring and training. Private screening contractors are expected to receive the same flexibilities as federal screener airports. These additional flexibilities will be measured by specific

success criteria and by ensuring TSA's goals for strong security and customer service are still being met at all airports.

c. What lessons did you learn from the comparison of private and federal screening programs? What changes will you make in TSA headquarters management of the screening program as a result of this study?

Answer: One the principal reasons for TSA completing an independent evaluation of the PP5 program was to identify lessons learned for incorporation into the Screening Partnership Program (Opt Out).

The BearingPoint study:

- Found that the private screening pilot airports met the Aviation and Transportation Security Act security by performing at the same level or better than federally screened airports
- Confirmed strong FSD management is a key factor that drives screening performance
- Confirmed that TSA has been successful in overseeing security operations at the five participating airports

TSA also asked BearingPoint, the independent evaluator, to identify ideas for possible program improvements. TSA is analyzing several of the program improvement ideas and plans to incorporate those that make sense. TSA already plans to incorporate the following program improvements:

- Increase decentralization and local empowerment across airports, particularly in the areas of assessment and screener technical training
- Improve communications and the documentation of program policies
- Clarify the roles and responsibilities of the TSA, FSD, airport director and private contractor
- Analyze performance measurement: work toward service level agreements and performance measures with more specific targets

As a result of the report, TSA is also reinstituting the FSD orientation program for newly appointed Federal Security Directors. The program will involve assigning each new FSD a mentor to provide guidance and support to new FSDs as they adapt to their new positions and environment.

BAGGAGE SCREENING

33. The Aviation and Transportation Security Act (ATSA) mandated the screening of all checked baggage using explosive detection systems by December 31, 2002. Congress subsequently authorized an extension for noncompliant airports until December 31, 2003. Almost two billion dollars have already been obligated for acquisition and installation of explosive detection systems for checked baggage screening at airports but TSA is still not

electronically screening 100 percent of all checked baggage and is relying on alternative means

a. When will TSA be able to screen all checked bags using explosive detection system (EDS) and explosive trace detection (ETD) without resorting to alternative means such as Positive Passenger Bag Match?

Answer: The TSA provides the status of those airports that have not achieved full electronic screening capabilities in a monthly-classified report to Congress. That report provides expected compliance dates. While TSA uses Congressionally approved mitigation procedures at the remaining airports, TSA sees a continuing need for use of mitigation procedures even if an airport has sufficient staffing and equipment capacity. There will be occasions when because of equipment maintenance needs, unexpected passenger load peaks and or unexpected staffing shortages that TSA will need to use Congressionally approved alternatives.

b. Is Positive Passenger Bag Match as effective as screening with EDS and ETD? Does bag match fully prevent a terrorist from placing a bomb on an aircraft if the terrorist is willing to die in the attack? Do you support continued use of Positive Passenger Bag Match?

Answer: As of today, checked baggage is being screened by electronic means in over 98% of our nation's airports. As mandated by both the Aviation and Transportation Security Act and Section 425 of the Homeland Security Act of 2002, alternative screening methods are used to screen each checked bag at the airports where all bags are not screened electronically. As you know, Congress approved these alternative means, which include hand searches, bomb-sniffing dogs and positive passenger bag match (PPBM). TSA's airport Federal Security Directors (FSDs) have been directed to work with the air carriers at their airport and develop a mitigation plan using these methods to screen checked baggage bags when explosive detection systems are not available or when the equipment reaches its maximum throughput capacity. That plan includes the option to use enhanced PPBM on a limited basis when all other screening options are not available.

I support PPBM as a risk mitigation method. Since no single safeguard can provide complete protection against terrorism, TSA has built and continues to strengthen an interlocking system of deterrents and risk mitigation strategies. PPBM is part of that system of systems. It provides a deterrent against terrorists who wish to attack without endangering their own lives, as well as inserting uncertainty into attempts to plan an attack against a commercial aircraft. Along with the other tools in our arsenal for screening baggage such as EDS and ETD, PPBM adds to the security of our aviation system.

As a result of the various methods approved for alternative means of screening, only a small and varying percentage of checked baggage is now subject only to PPBM. This method is a last resort used only when no other alternative screening methods are

available. This number will diminish as more of the remaining airports switch to electronic methods of screening. As you know, TSA is hard at work in ensuring that electronic screening is in place at all commercial airports. We submit a monthly classified report to Congress detailing the status of that effort.

c. Is "mitigation," an ETD technique that is used to speed up baggage screening by swiping as many as 6 pieces of checked luggage at one time with one cloth swab, an effective technique for ensuring that bags placed aboard passenger flights do not contain explosives?

Answer: TSA uses congressionally approved alternative screening procedures for checked baggage when the number of bags to be screened in a certain period of time exceeds either the equipment capacity or available staffing. TSA has permitted the use of an outside only ETD sampling of checked baggage of non-selectee passengers during these temporary periods of time, and has permitted its screeners to sample multiple bags with one sampling medium.

34. The President's fiscal year 2005 Budget proposes keeping the federal cost share for Letters of Intent (LOIs) for the development of in-line checked baggage systems at major airports at 75 percent rather than the 90 percent match required by the FAA reauthorization bill.

a. Please explain the rationale for this decision.

Answer: At the 75 percent cost share level, TSA can use its allocated funding to support current LOI airports as well as those airports that have not received an LOI but where additional equipment capacity is needed to accommodate increased passenger loads and new air carrier service. The 75 percent Federal funding level has been a long established cost share with larger airports under the Airport Improvement Program.

b. What would be the impact of providing a 90 percent match? Why do you think that the FAA reauthorization mandate for a 90 percent match does not apply to the LOIs signed by TSA?

Answer: At the 90 percent cost share level, TSA would have to limit remaining installation work needed at many non-LOI airports to ensure compliance with the 100 percent electronic checked baggage screening requirement during FY 2004 so that additional funding could be carried over into FY 2005 to make LOI payments.

The "Department of Homeland Security Appropriations Act, 2004," P.L. 108-90, provides that "none of the funds appropriated or otherwise made available by this or any other act may be obligated or expended to carry out provisions of section 44923(h) of title 49 United States Code." This proviso prohibits TSA to access funds authorized specifically for making grants under the special requirements of § 44923, including the requirement establishing a 90 percent Government cost share for certain projects "under this section." Therefore, TSA has issued LOIs for Atlanta and Phoenix airports under

separate authority previously established by § 367 Title II, Division I, of the Consolidated Appropriations Resolution, 2003, P.L. 108-7, which provides that the Government's share of project cost shall be 75 percent for a project at an airport having at least 0.25 percent of the total number of passenger boardings each year at all airports, and 90 percent for a project at any other airport.

c. What are TSA's long-term plans for supporting in-line checked baggage systems?

Answer: TSA is committed to supporting the efforts of those airports that are initiating designs for in-line screening solutions by providing technical expertise and guidance. However, TSA cannot commit to providing funding to support such systems. TSA will continue to focus its available funds on purchasing and installing EDS and ETD equipment at those airports that require additional equipment capacity to be compliant with the 100 percent electronic screening mandate for checked baggage. Increasing passenger loads, new air carrier service and airport terminal modifications and expansions, make 100% compliance a constantly shifting target.

35. The Homeland Security Act extended until December 31, 2003 the deadline by which TSA was required to screen all checked bags for explosives by machine, but even this extended deadline has not been met at all airports. The DHS IG reported in March 2004 that the barriers to meeting the deadline included not only delays in delivery or installation of electronic screening systems, but also factors such as ongoing construction and insufficient screening staff to operate the machines. What is your plan for achieving the goal of screening all checked bags for explosives electronically and when will this occur? What resources do you believe TSA will need to complete this task? Do you support hiring additional federal screeners for this purpose?

Answer: The TSA provides the status of those airports that have not achieved full electronic screening capabilities in a monthly-classified report to Congress. That report provides expected compliance dates. TSA is continuing to purchase and install additional EDS and ETD equipment, and hire additional screeners to operate that equipment at the affected airports.

When this equipment is installed, tested and ready, TSA will provide the necessary personnel to commence checked baggage screening operations within the limits of the overall national screener workforce cap of 45,000 FTE. We believe that we can address these requirements within the current statutory cap.

36. TSA has signed letters of intent (LOIs) with nine airports to provide funding to help defray the costs of installing permanent explosives detection systems (EDS) that are integrated with the airports' checked baggage conveyor systems. A TSA news release from February 2004 announcing the latest LOIs stated that the total amount of projected funding for these agreements was more than $955 million over 3 to 4 years. A March 2004 DHS IG report stated that 36 formal requests for LOIs had been received by TSA and at least another dozen inquiries had been made regarding such funding. TSA's FY 2005 Budget Request includes a total of $400 million for the purchase and installation of

EDS under the LOIs already signed as well as other costs such as the purchase of electronic trace detection machines.

a. If you are confirmed as Assistant Secretary, will you sign additional LOIs with airports?

Answer: Please see the answer to "36b." below.

b. How many additional airports seeking LOIs can be accommodated with TSA's FY2005 funding request?

Answer: The President's budget proposal to the Congress requests funding to support the eight currently signed LOIs. While LOI's are an important tool to assist airports in realizing efficiencies in handling checked baggage, TSA also pursues other mechanisms that provide EDS technology to the airports.

TSA's top priority is security, and consequently, TSA will focus its available funds for EDS at those airports that require additional funding in order to be compliant with the 100% electronic screening mandate for checked baggage. Changes to passenger throughputs, terminal modifications and airport expansions make fulfilling TSA's goal of 100% electronic baggage screening a constantly moving target. TSA continues to balance many competing priorities for available funds and will continue to review its priorities to maximize the utilization of the funds available.

At the current funding level, and applying the 75/25 cost share formula, TSA's FY 04 and FY 05 budget allocations for EDS installation can financially support:

- Reimbursement payments for the 8 existing LOIs (covering 9 airports)
- Installation and multiplexing of EDS equipment at the 9 LOI airports
- EDS installation work needed at 13 airports that are building in-line systems
- Using FY 03 FAA AIP grant money and EDS and ETD non-LOI installation work needed at airports to provide equipment capacity. The airports selected have a need for increased equipment capacity because of increased passenger loads and airport terminal expansion projects to support increases to air carrier service.

c. Will some airports that need LOIs to install integrated EDS not be able to receive federal funding under current funding request levels?

Answer: An additional 56 airports have expressed an interest in entering into an LOI with TSA for an in-line baggage screening solution. While TSA has not completed the evaluation of the various requests to accurately project potential costs, we continue to place top priority for our funding on ensuring compliance with the 100% electronic screening mandate.

d. If there is insufficient funding to support LOIs with all airports that need federal assistance to install integrated EDS, how will that affect your plan to meet the requirement to screen all checked bags electronically?

Answer: At the current funding level, and applying the 75/25 cost share formula, TSA can support the LOIs that have already been issued. While in-line screening solutions would provide for efficiencies associated with accomplishing electronic screening, TSA will be able to meet the requirement to screen all checked baggage using stand-alone screening configurations.

AIR CARGO

37. TSA largely relies on its known shipper program to ensure the safety of cargo on passenger aircraft. Please describe what safeguards exist to keep the Known Shipper Program from being exploited by terrorists. Please describe what additional steps, other than the Known Shipper Program, TSA plans to implement to provide for the security of cargo on passenger flights.

Answer: The Known Shipper Program has been a key element in air cargo security for over 20 years. The Known Shipper Program is an information-based approach to cargo security through the identification of strong commercial relationships. The Known-Shipper program is utilized by passenger air carriers, Indirect Air Carriers (IACs, or freight forwarders), and all-cargo carriers who transfer cargo to passenger planes. Known Shipper has previously operated in a decentralized mode, with each carrier and IAC responsible for maintaining its own separate database of known shippers. In an effort to strengthen the program and to reduce its vulnerability to exploitation, TSA has developed and implemented a centralized Known Shipper database that allows all participating carriers to verify the known status of a particular shipper. Shippers in the Known Shipper database are verified against a variety of watch lists and terrorist data and their status is centrally recorded. Shippers accepted in the program are deemed to pose a lower risk and therefore allowed to transport cargo on passenger aircraft. More than 450,000 known shippers are already included in the database, and the system is currently averaging about 1,000 inquiries a day. Because the database is now centralized and managed by TSA, it can easily be modified to respond to new threats to aviation presented by international terrorism.

In November 2003, TSA issued security directives that require random inspection of air cargo on passenger aircraft on flights within, into, and out of the United States. The layered approach to securing cargo carried on passenger carriers may include: physical screening (including TSA screeners when available), x-ray, inspections using ETD, K-9 screening, or explosives detection system. The inspections are to be conducted by the air carrier, with TSA ensuring that the inspections are conducted properly. Screening on passenger carriers is in accordance with procedures already in the aircraft operator's security program. To assist in that effort, we are in the process of completing the hiring of an additional 100 TSA cargo security inspectors who are responsible for ensuring industry compliance with the new screening requirements.

In TSA's FY 05 budget request, we have requested $55 million to develop new technologies for inspecting cargo for explosives, radiation, chemical and biological agents, and other dangerous substances.

Finally, the Department is currently reviewing TSA's proposed Air Cargo Rule which would codify many of the security changes applied since 9-11 and would impose additional security measures across the air cargo industry. The rule incorporates many of the industry recommendations from the Aviation Security Advisory Committee (ASAC) process as well as additional measures deemed necessary based on the Department's assessment of threat and vulnerability in the air cargo environment.

38. Please describe the steps TSA has taken, and plans to take to provide for greater security procedures for indirect air carriers.

Answer: On May 3, 2004 TSA rolled out an IAC database that allows TSA to factor additional security criteria into the vetting process by requiring Indirect Air Carriers to provide corporate information electronically. TSA will be able to legitimize the applicant through a check of publicly available corporate records, and to cross check those records against the various criminal and terrorist databases. This process provides better vetting of IACs who are applying for either approval or renewal of their certificates, and it also strengthens the decertification process. The system will automatically delete any IAC who does not reply to the 30-day re-certification alert and it also reduces the time spent by Aviation Security Inspectors re-certifying IAC's.

39. You have described your intent to develop a cargo pre-screening program to identify high-risk cargo and to ensure that cargo is inspected. Where does the development of such a program stand?

Answer: TSA plans to deploy a cargo prescreening system to target individual shipments for inspection based on the likelihood that they pose a threat to the aircraft either through the introduction of an Improvised Explosive Device (IED) with the intent to destroy the aircraft or a stowaway with the aim of hijacking the aircraft for use as a weapon. This system will be similar to that used by U.S. Customs and Border Protection to prioritize imports and exports for inspection; however, it will be tailored to deny a terrorist the opportunity to introduce an Improvised Explosive Devise or hijacker into the aircraft. These efforts support the Department's goal to pre-screen 100% of cargo shipments and to require additional inspection for cargo identified as high-risk.

TSA will utilize information obtained from the involved parties through its Known Shipper and IAC validation programs as well as information specific to each individual shipment that will be provided by either an aircraft operator or indirect air carrier. The exact content and timing has yet to be determined. This information will be processed through analytical tools and compared against relevant threat data such as compliance records and intelligence information. From this assessment, TSA will electronically produce a risk score. Shipments above a certain score will be identified as elevated-risk.

Upon a shipment's identification as elevated-risk, the carrier would be required to inspect that shipment to determine whether it poses an actual threat and whether law enforcement needs to be notified. This kind of public-private partnership is the most effective solution available as TSA does not possess, nor does it see the need for, a federal cargo inspection force comparable to that which exists for passenger screening. By placing this responsibility with the carrier, the important inspection process can be integrated into the supply chain, instead of adding a potential bottleneck that would likely slow interstate and international commerce.

Earlier this year TSA issued a Request for Information to interested parties seeking information from industry on existing and emerging technologies that will aid TSA in the development of this system. The RFI period closed on April 30 and TSA staff are now engaged in the process of reviewing the submitted proposals and anticipate having a working prototype by the end of FY 2005.

40. How is the information gathered through the Known Shipper Program being coordinated with information gathered through other DHS programs, such as C-TPAT and FAST? Does a shipper that operates by land, air, and sea have to enroll separately in each of the three programs? What steps are being taken to consolidate and cross reference information from all three programs to increase accuracy and avoid unnecessary duplication?

Answer: Since June 2003 TSA has worked closely with U.S. Customs and Border Protection (CBP) to leverage resources, identify areas for information and technology sharing, and strengthen the security of the air cargo supply chain. After an exchange of program overviews, it was determined that the Customs-Trade Partnership Against Terrorism (C-TPAT), which currently has more than 3500 participants, including major U.S. importers and major air passenger carriers and the Known Shipper Program, which currently has 250 air carriers and 3,800 Indirect Air Carriers (IAC's), share common ground. When coupled with enhancements to the Known Shipper Program, these increases in supply chain security will significantly reduce the chances that an explosive device or other destructive substance or item could be loaded on a commercial passenger airplane as cargo.

At this time, shippers who operate by land, air and sea have to enroll separately in the Known Shipper Program, C-TPAT and the Free and Secure Trade program (FAST). TSA will conduct a connectivity and interface pilot between the Known Shipper database and the C-TPAT program from September 2004 and March 2005.

CHECKPOINT SUPPORT

41. The President's fiscal year 2005 budget includes $86M for checkpoint support, which we understand to include checkpoint reconfiguration, maintenance and replacement of checkpoint equipment, testing and deployment of new technology, and video

surveillance. Do you believe that the Administration's request is sufficient to meet these needs?

Answer: TSA is committed to providing the appropriate amount of technological support to the screening workforce at the passenger checkpoint. Checkpoint Support is comprised of the many technology-related activities that do this, including checkpoint reconfiguration; the purchase, installation, and maintenance of checkpoint equipment; and electronic surveillance. The breakout of TSA's budget requests for checkpoint support for FY 2004 and FY 2005 is captured below:

(dollars in millions)	FY 2004	FY 2005
Checkpoint equipment purchase	$30.0	$30.0
Checkpoint equipment maintenance	$14.0	$30.0
Checkpoint reconfiguration	$ 4.0	$16.0
Electronic surveillance	$14.0	$10.0

RESEARCH AND DEVELOPMENT

42. Do you think that research and development for homeland security technologies should be centralized in one place in the Department of Homeland Security or do you believe that separate entities within the Department, such as TSA, should continue their own research and development programs?

Answer: TSA is closely coordinating with the Science and Technology directorate on R&D to ensure effective use of resources and to leverage efforts. Whether R&D is centralized or continues to be conducted within separate entities, the critical issue is ensuring that the R&D meet the constant demand for improved technology performance and the very specific detection capabilities needed to support TSA's mission.

43. What progress has TSA made in the development of next generation explosive detection systems? What impact will these improved machines have on the number of bags that can be screened in an hour and thus the number of screeners required for baggage screening? Would more funding of these efforts accelerate this development or are there simply technical hurdles that require time?

Answer: In support of our efforts to identify the next generation of explosives detection technology for checked baggage, we have both short term and longer-term efforts underway in R&D. The Phoenix Project is a shorter-term effort (1-3 years) that focuses on three areas:

- Significant improvements to our currently deployed systems that will lower alarm rates, while increasing throughput capacity, detection capabilities and reliability. The improvements that will lower alarm rates while increasing detection capabilities will require that fewer bags be subjected to secondary screening, therefore, less staffing will be needed to support secondary screening;

- Combining emerging technologies such as quadruple resonance and x-ray diffraction with our current systems to expand capabilities; and

- Evolutionary new systems taking advantage of technological improvements and advancements in computed tomography.

There are a total of seven individual projects underway in Phoenix, each with its own required development timetable/schedule. We anticipate that the first field testing of a Phoenix solution could occur in the late 2004 timeframe, with the other solutions following throughout 2005 and early 2006.

TSA has been working with one vendor in the development of an EDS technology that is much smaller and significantly less expensive than the currently certified EDS units, which uses computed tomography. This technology is scheduled to undergo laboratory certification testing in June 2004. This will afford TSA an option for operations with lower throughput demands.

The longer-term effort in checked baggage in the Manhattan II Project (3-5 years and beyond). The initial announcement for this project was published on April 16, 2004. The intent is to award multiple proof-of-concept efforts, which will last approximately one year. Upon completion of this phase, we will evaluate the results and award system development contract(s) towards those concepts and technologies that are proven and demonstrated. Depending on the maturity of the technology, the timetable/schedule for system development under Manhattan II could vary.

44. Several local transportation agencies and national groups have indicated a strong need for research and development of technologies that can detect chemical, biological and other attacks on transportation systems. They have also called for technologies that can help systems respond quickly to an attack to ensure minimal impact and quick restoration of service. These agencies and other actors also have indicated a need for a Federal clearinghouse to help guide local decision-making on technology purchases. (See *Mass Transit: Federal Government Could Help Transit Agencies Address Security Challenges,* GAO-03-263)

    a. What are your plans to carry out research, development and deployment of detection technologies?

Answer: With research and development efforts, time is needed to determine technology capabilities for meeting TSA's operational needs and to determine or make recommendations regarding other applications. TSA and S&T are working with funding allocated for research and development projects to improve and advance technological solutions.

As noted above, for checked baggage, we have both short term and longer-term efforts underway in R&D. The Phoenix Project is our shorter-term effort (1-3 years) that focuses on three areas:

- Significant improvements to our currently deployed systems;
- Combining emerging technologies such as quadruple resonance and x-ray diffraction with our current systems; and,
- Developing evolutionary new systems taking advantage of technological improvements and advancements in computed tomography.

There are a total of seven individual projects underway in Phoenix, each with its own required development timetable/schedule. We anticipate that the first field testing of a Phoenix solution could occur in the late 2004 timeframe, with other systems following throughout 2005 and early 2006.

The longer-term effort in checked baggage screening is the Manhattan II Project (3-5 years and beyond). The initial announcement for this project was published on April 16, 2004. The intent is to award multiple proof-of-concept grants, which will last approximately one year each. Upon completion of this phase, we will evaluate the results and award system development contract(s) to those organizations with concepts and technologies that are proven and demonstrated. Depending on the maturity of the technology, the timetable/schedule for system development under Manhattan II will vary.

For cargo security, TSA's research and development efforts to identify appropriate technologies for screening air cargo are well underway. TSA believes that its recent Market Survey and Broad Agency Announcement for potential technology manufacturers has provided TSA with a sound base for pursuing development of multiple technologies in support of air cargo screening. While currently available technologies will be subjected to operational testing and evaluation for cargo screening, new technologies will not likely produce a testable prototype for 18 to 24 months.

For checkpoint security, TSA's research and development program is designed to develop sensor fusion at our screening checkpoints to combine technology capabilities into single units. Currently, TSA is evaluating the capabilities of explosives detection portals, which will be pilot tested at a number of airports during the 3rd quarter of FY 2004. While this effort is underway, TSA is working towards combining capabilities of explosives and weapons detection systems and devices. One of the research and development projects underway is the use of body imaging technology for screening, which detects anomalies on a person's body to include those created by concealed weapons and explosives. While this technology is not yet ready for operational testing due to privacy issues, which must first be resolved, it is a technology solution that could serve two purposes in the screening of persons.

TSA has developed a "Roadmap" for the operational testing and evaluation of checkpoint technologies to improve TSA's ability to detect explosives being carried on persons and in carry-on baggage. Below is a list of the explosives detection technologies to be pilot tested at airports and the timeframe in which that testing will be accomplished:

- Explosives Detection Portals – continued development and pilot deployment in the 3rd quarter of FY 04;
- Document Scanners – continued development and pilot deployment in the 3rd quarter of FY 04;
- Cast & Prosthetic Device Scanners – continued deployment and pilot deployment in the 3rd quarter of FY 04;
- Explosives detection technology for screening liquids – establish the performance metrics for this technology and solicit vendors of existing technologies to participate in an evaluation against this qualification standard; and,
- Explosives detection systems (EDS) for carry-on baggage – define performance metrics and solicit vendor participation 3rd quarter of FY 04.

b. Will TSA undertake research to help improve the basic infrastructure of systems – architecture, materials and construction methods, for example - to enhance facilities and mitigate the effects of terrorist attacks?

Answer: TSA has undertaken several projects to improve infrastructure security:

- 20 Airport Access Control Pilot Program – As required by the Aviation and Transportation Security Act, we have initiated 8 pilot projects to operationally test and evaluate access control technologies, to including those using biometrics. TSA will initiate and complete 10 pilot program projects by the end of CY 04. Information obtained during these projects will be shared with other Federal agencies, as well as industry representatives to provide them with information about specific technology capabilities as they design systems to protect their facilities.
- Biometrics Standards Development – We are continuing research and development to establish standards for biometric systems through ongoing pilot programs and laboratory efforts. These technologies will find applications in our Transportation Worker Identification Credential (TWIC) and registered traveler programs, as well as any other system/program area that will require use of biometric technology.

- Seaports and other Transportation Facilities - We will continue R&D efforts to determine applicability of aviation security solutions and systems to protect other transportation facilities and conveyances.

c. What will you do to encourage research and develop means to improve emergency decision making and communications capabilities?

Answer: Please see the answer immediately below (44.d.).

d. Will you establish a clearinghouse mechanism to ensure that transportation system operators can find out what security-related technologies are available or in development?

Answer: TSA will work with the other DHS elements to determine how best to communicate results of TSA's research and development efforts related to security technologies, so that these results can benefit any and all entities that must use such technologies to fulfill their mission of protecting the Nation's transportation infrastructure. Until a clearinghouse type of mechanism is in place, TSA will continue to reach out to its stakeholders through established methods of communications.

PORT SECURITY GRANTS

45. In its fiscal year 2005 budget, the Administration requested only $46 million for port security grants. This funding level is nearly $100 million less than fiscal year 2004. In addition, the Administration's budget proposes to transfer port security grants from TSA to Office of State and Local Government Coordination and Preparedness (SLGCP) and include these grants in the Urban Area Security Initiative (UASI). As you know, UASI provides resources in a very different manner than TSA's port security program. For example, UASI port security grants only target ports in urban areas. Moreover, instead of accepting applications, UASI port security grants designate specific areas without regard to considering requests from a wide range of ports.

There is concern about the administration's proposal to decrease the amount of port security funding given the considerable need as a result of MTSA requirements and the many vulnerabilities of our ports. There are also concerns that many ports would appear to be ineligible for the funding since they are not in urban areas. Making these funds available and requesting applications helps smaller ports identify vulnerabilities of which DHS may not be aware.

a. Do you support consolidating port security grants into the UASI program?

b. What do you think will be the effect of consolidating these grants into UASI?

c. What do you believe needs to be done to ensure that all ports are eligible for port security grants?

d. How should TSA be involved in the program?

e. If the grants are moved to SLGCP how will they be administered?

f. Will SLGCP have the expertise to make appropriate decisions regarding the allocation of these grants?

Responses to Questions 45a-f, appear in the consolidated answer below:

Answer (a. – f.): As initial clarification, the port security grant program is not going to be consolidated into the UASI program. The move to create a one stop shop for grants is based upon input from the user or grantee community and is designed to enhance coordination of the multitude of preparedness and security grants currently administered by the Department (ODP, FEMA and TSA). The one-stop shop consolidation will allow DHS to gain a global perspective on all of the grants to ensure that redundancies are minimized, funds are directed to the highest best use and DHS can proactively make recommendations to states, localities and other recipients on mutual aid and dual use opportunities. We expect that this will be a seamless transfer that will be transparent to the grantees.

Final policy responsibility for grant guidance and grant distribution will reside with the Office of State and Local Government Coordination & Preparedness (SLGCP). SLGCP will create a distinct office dedicated specifically to transportation related grants. This new office will work closely with TSA and the other appropriate agencies within DHS and across the Federal government in developing transportation security grant policy.

As stipulated in the initial appropriations language, (Department of Defense and Emergency Supplemental Appropriations for Recovery From and Response to Terrorist Attacks on the United States Act, 2002 (P.L. 107-117) and subsequent appropriations language, port security grant funds are dispersed through a competitive grant process to critical national seaports. The current process incorporates a multi-level, interagency review, which ensures that funds go to the highest national security needs.

Responsibility for all grants previously under TSA's purview, including port security grants, officially moved to SLGCP on May 16, 2004. Four TSA personnel involved in program management of these grants were detailed to SLGCP at that time. It is my understanding that SLGCP will administer round 4 of the port security grants the same way TSA did for the first 3 rounds. TSA will continue to make available, upon request, its subject matter experts for any of the transportation security grants that SLGCP now administers, including port security grants.

It is important to understand that USAI grant funds were administered by SLGCP and not TSA. Though ODP did use some UASI grant money for port security purposes at one time, I am not aware of any plans that they may, or may not, have to consolidate the port security grants into their UASI grant program. If it is the desire of Congress that all ports be eligible for port security grants, the eligibility language in the appropriations bill will

have to be expanded from the current constraint of only "critical national seaports" being eligible.

CONTAINER SECURITY

46. Container security is often viewed as a component or subset of port security. However, the integrity of a container is part of a larger, inter-modal transportation security effort, which utilizes sea-borne vessels, freight trains and trucks to move goods all around the world. The Department of Homeland Security has initiated programs to inspect containers based on a risk assessment, to track and monitor individual containers, and to use non-intrusive detection equipment to screen containers at various points in the supply chain. TSA, the Bureau of Customs and Border Protection (CBP), and even the Coast Guard have contributed to these and other container security programs.

a. What do you believe should be TSA's role in developing and administering inter-modal container security programs?

Answer: The Department of Homeland Security (DHS) was established to coordinate all of the efforts of various agencies in securing our homeland. In fulfilling this mission, it builds on the strengths and expertise of all of the agencies that work with each mode of transportation.

The U.S. Coast Guard (USCG) is the lead agency for maritime security issues because it has decades of experience and powerful assets focused on securing the maritime domain. With this framework, however, TSA has been directed to support the USCG in the execution of certain responsibilities where leveraging of TSA's expertise may be appropriate, including development of maritime passenger screening standards and transportation worker credentials.

CBP is the lead entity within DHS for execution of cargo container security inspections in the international shipping environment. However, recognizing the intermodal nature of cargo shipments, the Border and Transportation Security (BTS) Directorate has been delegated authority and responsibility for developing a secure system of transportation for intermodal cargo shipments, and container security performance standards. BTS is supported by both CBP and TSA in execution of these responsibilities.

In addition, the USCG works with TSA, CBP, and other Federal agencies (e.g., DOT's MARAD) as team members to be used to complement USCG efforts within the overall maritime security regime, including development of USCG's comprehensive regulatory package implementing the bulk of the Maritime Transportation Security Act (MTSA) requirements, and provision of security for the maiden voyage visit of the Queen Mary 2.

Finally, all elements of DHS work closely and collaborate on a daily basis with Information Analysis and Infrastructure Protection (IAIP) on issues related to surface transportation security. IAIP shares intelligence and threat analysis daily with all DHS entities and other relevant stakeholders. Since the Madrid bombings, DHS initiated a

working group designed to develop specific operational Courses of Action (COAs), led by BTS, and including representatives from TSA, IAIP and DOT Modal Administrations.

b. To what extent has TSA coordinated with CBP, and even the Coast Guard, to help ensure the effectiveness of the various container security programs?

Answer: The Department of Homeland Security was created to maximize the Federal Government's interagency coordination, and TSA has embraced this mission and places a key role in fostering interagency cooperation. For example:

TSA is collaborating with U.S. Customs and Border Protection (CBP) and USCG to conduct a program analysis of current cargo security programs under the leadership of Border and Transportation Security. The goal of this analysis is to investigate the various cargo security programs within DHS and to measure their effectiveness. The analysis will be presented to the Commercial Operations Advisory Committee (COAC) Subcommittee on the Implementation of the Maritime Transportation Security Act (MTSA), which will in turn make recommendations regarding the effectiveness of cargo security programs from a commercial perspective. This subcommittee of which TSA, CBP, and USCG are members is also tasked with developing performance standards for the physical security of freight containers.

Operation Safe Commerce is an interagency program with TSA, CBP and the Department of Transportation acting as co-chairs of the program and TSA serving as the National Coordinator. Further representatives from USCG, Department of Defense, Department of State, and Department of Commerce are also represented on the program's Executive Steering Committee.

TSA continues to work daily to coordinate with CBP and Coast Guard. Supply chain security is a broad and complex issue that necessitates the combined efforts of all of the agencies involved in transportation and cargo security. TSA's role as the DHS designated Sector Specific Agency (SSA) responsible for the security of the transportation sector has meant that interagency coordination must be a priority. TSA's mandate to secure all modes of transportation as well as TSA's ability to use Security Directives to address security concerns gives TSA a unique ability to work with the Coast Guard and CBP to meet the goal of a secure transportation system.

GENERAL AVIATION

47. In testimony before the Senate Commerce Committee Subcommittee on Aviation on March 30, 2004, GAO criticized TSA for taking "limited action to improve general aviation security, leaving general aviation far more open and potentially vulnerable than commercial aviation." *Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts*, GAO-04-592T. Weaknesses noted by GAO include: general aviation pilots and passengers are not screened before takeoff, the contents of general aviation planes are not screened at any point, about 70 aircraft have been stolen from general

aviation airports in the last 5 years and could be used for terrorist activity, and crop dusters could be used to spread biological or chemical agents.

a. Do you believe that TSA needs to take steps to improve general aviation security? If so, please state what actions you will take if you are confirmed as Assistant Secretary.

Answer: TSA is fully engaged in improving general aviation (GA) security. Since there is no silver bullet that can guarantee security, a layered, flexible approach is critical to ensure that all segments of the aviation sector are secure. In concert with our overarching strategy, TSA is taking a threat-based, risk-managed approach to securing the full spectrum of general aviation, including private charter and corporate/business aviation operations.

TSA has taken a number of steps to improve GA security. The agency has implemented regulatory regimes for large and small private charter operators, a segment of the general aviation industry not previously regulated for security purposes. Our GA security efforts include partnering with the Aircraft Owners and Pilots Association (AOPA) to implement a nationwide Airport Watch Program that is anchored by a federally-funded and operated GA Hotline. We have also partnered with the National Business Aviation Association on a pilot project at three major corporate airports. This initiative, known internally as the TSA Access Certificate (TSAAC) pilot program, requires corporate operators to meet and maintain enhanced security standards.

There is always more that can be done, and we cannot be complacent about security measures that we have taken to date. I am acutely aware that, as TSA has worked diligently to close security gaps in the commercial aviation sector, GA may appear relatively more vulnerable to exploitation by terrorists. Therefore, a number of additional projects are on the horizon for GA. First, TSA is currently working on a self-assessment tool that can be used to evaluate risk at GA airports across the country. That tool will be rolled out to all 5,400 public use GA airports in summer 2004. Second, development is underway for a 5-year strategic plan for GA that is intended to cover 2005 – 2009. Third, TSA is planning a communications process that will enable TSA to communicate quickly and efficiently with GA airports nationwide. Fourth, TSA is undertaking a headquarters-led inspection process for the more than 3,500 flight schools and training centers. Fifth, later this year TSA will provide background checks on aliens attending flight schools in the United States following the transfer of the program from the Department of Justice.

Finally, Federal Security Directors (FSD) are conducting outreach activities at GA airports within the vicinity of the commercial service airport for which they have responsibility. In this role the FSDs will provide GA airport owners and operators with guidance, assistance, and advice on security measures at their facilities and other pertinent security information. These relationships will facilitate communication and help ensure that TSA is knowledgeable about the changing needs of the GA community.

b. TSA's Working Group on general aviation issued recommended guidelines for general aviation airport security in October 2003. The Working Group report noted

that one barrier to improving general aviation security was the lack of funding. Do you plan to request funding to help general aviation operators improve security?

Answer: TSA is constantly reevaluating its needs with regard to general aviation security. These needs are frequently driven by emerging threats and intelligence. TSA will make funding decisions through a threat-based, risk-managed approach and will allocate resources appropriately as they become available. TSA will continue to consult with Congress on efforts to safeguard general aviation.

c. TSA released security guidelines for general aviation airports on May 17, 2004, but these guidelines are merely suggestions for security measures that general aviation airports could implement. What steps will you take to ensure that appropriate security measures are implemented by general aviation airports and aircraft owners?

Answer: Consistent with its work in other modes, TSA pursues its GA efforts in partnership with State, local, and private industry stakeholders. TSA has been working closely with its strategic partners within the industry to develop effective and reasonable procedures to enhance GA security. Our philosophy, which is embedded throughout the guidelines document, is to define an appropriate level of security commensurate with the varying levels of risk at different types of GA airports. TSA believes that the measures taken towards GA are consistent with those efforts that have been implemented in other comparable modes of transportation.

The security enhancements suggested in the Information Publication (IP) were developed in strong coordination with stakeholders, who were very supportive of this effort. Prior to the publication of this document, many States were developing their own sets of security guidelines and requirements for GA airports; however, they clearly indicated that they would prefer receiving a set of Federally-endorsed measures that would be implemented nationally. The National Association of State Aviation Officials actively participated in creating these guidelines, and we expect the States will encourage their GA airports to implement appropriate security measures. We also believe that development of these Federal standards will provide a baseline that States will use to allocate resources for GA airport security improvements. Additionally, we are conducting extensive outreach efforts through TSA's Federal Security Directors to ensure that all GA airport managers are aware of and have access to the security guidelines document. Early reports have indicated that the IP measures are being adopted by the GA community.

It is important to note that there is a heightened sense of security awareness within the GA community. General aviation today does not look like it did on September 10, 2001. Many operators and airports have invested significant amounts of money in tangible security enhancements such as fencing, access controls, surveillance equipment, lighting, signage, and a variety of other measures. The efforts undertaken in partnership with the general aviation community have significantly raised the bar for security at GA airports.

PERIMETER SECURITY

48. The Aviation and Transportation Security Act that established the Transportation Security Administration (TSA) directed the agency to improve the security of airline passenger and baggage screening activities, activities for which TSA has direct responsibility. The law also directed the agency to work with airports to improve the security of airport perimeters (such as airfield fencing and access gates); the adequacy of controls restricting unauthorized access to secured areas (such as building entry ways leading to aircraft); and security measures pertaining to individuals who work at airports. Recent media reports of security breaches and other illegal activities, such as drug smuggling, taking place at some airports highlight the importance of strengthening security in these areas. The Department of Transportation's Inspector General reported last year that TSA had not fully addressed requirements related to controlling access at airports and the GAO has issued a report assessing the status of the agency's efforts in this area.

a. As we approach the 3-year anniversary of the Act and the agency continues to face new challenges, what steps should the agency take to ensure that these existing legislative requirements are met?

Answer: The Aviation and Transportation Security Act (ATSA) of 2001 required the establishment of pilot programs at no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secured areas of the airports. ATSA also states that the technologies to be evaluated under the pilot programs may include, among others, biometric technologies. To meet this requirement, TSA has developed a two-phase pilot program, for which the first eight airports have been recently selected and announced, and the final two will be announced in the very near future, bringing the total to ten airports for Phase I. Phase I includes testing of various off-the-shelf technologies, including biometric technologies, under a variety of real-world operational environments. Phase I projects will be completed by December 2004. Based on analysis of Phase I projects, TSA will then determine which technologies will be evaluated in the ten different Phase II airports.

After Phase I and Phase II are both completed, information gathered during these pilot projects will be made available to appropriate airport and aviation industry representatives so that they may make informed decisions when designing access control systems to meet their security and regulatory needs. TSA has coordinated this effort with other DHS entities, such as US-VISIT, to leverage their expertise in biometrics, for example.

TSA has also issued 19 grants, totaling over $16 million to airports to fund pilot projects to improve airport terminal security. Of the 19 grants projects, at least 9 are associated with improvements to perimeter security protection and preventing unauthorized access to airport-restricted areas.

b. Is there a need to improve the agency's communications with the Congress on the status of its efforts to address these requirements? If so, how could this be best achieved?

Answer: TSA is proud of the relationship it is building with Congress. As the agency evolves, it continues to strive to improve that relationship and to further establish strong lines of communication. It is critical that TSA be responsive to the needs of its authorizing and appropriating committees as well as to the needs of individual Senators and Members of the House of Representatives. The key to strong communication is continual dialogue with respect to TSA's efforts and ongoing mission and I am committed to promoting and strengthening that dialogue with Congress. In terms of ATSA and other statutory requirements, I believe it to be of the utmost importance that we continue to ensure our oversight committees are aware of TSA's progress. Through TSA's Office of Legislative Affairs, the Agency prioritizes communication with Congress via notification, correspondence, briefings, and meetings. As with all of our efforts, TSA is open to interactions with Congress and looks forward to providing Congressional Members and their staffs information regarding TSA's work on perimeter security to date.

49. A report recently released by GAO (GAO-04-728) noted that TSA has not fully met all of the requirements in the Aviation and Transportation Security Act of 2001 (ATSA) regarding airport perimeter security, access controls on access to secure areas, and risks posed by airport workers with access to secure areas. In some cases, GAO noted that TSA has not begun to address these issues.

a. GAO's report stated that TSA suspended its security compliance and vulnerability assessments of threats to airport security in January 2004. However, TSA has indicated that it has resumed these assessments. Is this accurate? If not, do you believe that TSA should recommence these assessments? If so, what is TSA's schedule for completing these evaluations? How will TSA use the information it compiles to improve security and prioritize security needs?

Answer: Compliance inspections at commercial airports were not halted at that time. In fact, as GAO reported, we revised our approach to reviewing airport operator compliance with security regulations beginning in FY 04. This new inspection process uses risk management principles that consider threat factors, local security issues, and input from airport operators and law enforcement to target key vulnerabilities and critical assets. The FSD at each airport is responsible for determining the scope and emphasis of the inspections, as well as managing local TSA inspection staff. This new approach is a collaborative process intended to identify the root causes of security problems, develop solutions with airport operators, and focus the use of civil enforcement actions on the most serious security risks revealed by TSA's inspections.

As part of our focus on improved perimeter security, TSA conducts assessments to identify vulnerable areas and needed security measures. As GAO correctly noted in its report, TSA redirected resources from assessments using the Transportation Risk

Assessment and Vulnerability Evaluation (TRAVEL) tool to conduct MANPADS assessments that were considered a higher priority at the time. Although resources were temporarily redirected from the TRAVEL to MANPADS assessments, a substantial number of compliance inspections were performed during this time, particularly in the areas of access control and access media. TSA's active completion of these MANPADS assessments ultimately provided valuable information for inclusion in broader airport perimeter security assessments at the airports at which they were conducted, helping us to fulfill our compliance inspection plan and develop the self assessment tool for aviation.

TSA initiated Joint TSA/FBI assessments in May 2004. These assessments are focused on airports surrounding all National Special Security Events and will also be applied at critical commercial airports based on threat. The application of this tool will allow TSA to leverage existing FBI resources and knowledge base to better assess security gaps and vulnerabilities at particular airports.

TSA/FBI assessments have been completed at the Brunswick, GA and Savannah, GA airports in support of the G8 conference. Joint assessments for the Boston, Manchester, and Providence airports were completed in June 2004 in support of the Democratic National Convention. Joint assessments of the New York-area airports New York JFK, New York LaGuardia, and Newark, NJ airports are scheduled in July in support of the Republican National Convention.

The information from the joint assessments is being captured in the TSA Transportation Security Risk Model (TSARM) web-based tool. These assessments will result in the gathering of baseline security system information on commercial airports. The tool will be made available to all Federal Security Directors in September 2004 and data gathering will occur through the second quarter of FY2005. TSA will use the information gathered through this process to analyze baseline security system effectiveness throughout the Nation's airports. Analysis will focus on areas of weakness and will be used to prioritize TSA's security enhancement efforts. Results of the assessments are also provided to the FSD and airport operator along with recommendations for improvement, enhancements, and suggested countermeasures.

TSA has designated all Category X Airports as nationally-critical. TSA has also completed a Criticality analysis of the Category I commercial airports. The Category X and nationally-critical Category I airports will be the focus of TSA-led, on-site, facilitated vulnerability assessments using the TSA Transportation Risk Assessment and Vulnerability Evaluation (TRAVEL) tool. TSA is in process of upgrading this tool and on-site assessments of nationally-critical airports will begin in September 2004.

In addition to these government facilitated assessments, a self-assessment tool will be made available to airports that are deemed less critical which focus on prevention and mitigation of a base array of threat scenarios developed for various categories of transportation modes.

As part of our overall strategy to strengthen security of the aviation system, our analysis and evaluation of the results from the security evaluations, various assessments, and compliance inspections will be used to assess priorities and allocate resources to those areas that we believe require additional security measures to close identified gaps.

b. The report also noted that airports need TSA to provide guidance on commercially available technology to improve perimeter security and access controls to secure areas, as it is required to do under ATSA. Airport operators stated to GAO that getting this information from TSA will help them reduce the costs of determining what technologies are available and best meet their needs, to ensure that limited airport resources are used in the most effective way. What steps will you take as Assistant Secretary to conduct technology assessments, compile the results with those of airports that have done some testing on their own, and communicate the results to airport operators?

Answer: It is important that TSA develops and deploys new technology to make our security operations more effective, more efficient, less time consuming, and less costly. Working closely with the Science & Technology Directorate of DHS, TSA has established an ambitious program to develop, test, and deploy security technologies and use technology to enhance human performance. TSA is actively assessing technologies and has provided guidance to FSDs and airport operators on security technologies so that they may make informed decisions. Additionally, TSA has developed a number of guides to assist operators in selecting and deploying commercially available security technologies, including reports with subjects such as perimeter security design, biometrics at domestic airports, and technology to address tailgating and piggybacking.

ATSA required the establishment of pilot programs at no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secured areas of the airports. ATSA also states that the technologies to be evaluated under the pilot programs may include, among others, biometric technologies. To meet this requirement, TSA developed and is implementing a two-phase pilot program. Phase I, currently underway, includes testing of various off-the-shelf technologies, including biometric technologies, under a variety of real-world operational environments. Based on that analysis, TSA will then determine which technologies will be evaluated in the Phase II airports to begin in the fall of 2004. The pilot programs will focus on identifying the operational payoffs achievable through increased usage of biometrics, as well as other technologies. TSA has coordinated this effort with other DHS entities, such as US-VISIT, to leverage their expertise in biometrics, for example.

c. In addition, the report addressed the limitations of relying on one time fingerprint-based checks to determine whether airport workers should be permitted access to secure areas. What are your plans, if any, for addressing these limitations noted by GAO and for implementing ATSA's requirement to screen all airport workers before entering secure airport areas?

Answer: TSA is actively strengthening safeguards regarding access to Security Identification Display Area (SIDA) and sterile areas of our Nation's airports. Approximately 1.2 million aviation personnel (airport, airline and vendor employees, etc.) work in U.S. airports. More than 90% of these employees work in the Security

Identification Display Area (SIDA) because they require access to aircraft to load luggage and cargo, provide catering services, fuel airplanes, perform maintenance, or serve as flight crew. About 10% of workers require access only to the sterile area, which is located past the screening checkpoint. The sheer quantity of airport workers with SIDA credentials and the fact that they would have access to a wide variety of tools and equipment within the SIDA area preclude any simplistic solutions. TSA's security strategy uses a "system of systems" approach whereby each security ring contributes to TSA's overall security system but the overall system does not rely exclusively on any one component. In other words, the different security components complement and reinforce each other.

In applying this "system of systems" strategy to securing SIDA and sterile area access, TSA is in the process of strengthening background checks. TSA currently requires fingerprint-based criminal history record checks of all airline and airport workers who have access to SIDA and vendor employees who work in the sterile area of an airport. In June 2004, TSA will begin conducting enhanced background checks on all commercial aviation workers in the U.S. who have access to the secure and sterile areas of our Nation's airports. This initiative will also include vetting new employees as they join the workforce, and the integration of newly available threat information. These enhanced checks will include advanced analysis of the best available information to determine whether an individual poses a potential terrorist threat. This initiative will focus on preventing known terrorists from gaining credentials allowing access to SIDA and sterile areas, thereby diminishing threats to our aviation system.

While TSA considers physically screening all aviation workers to be impractical at this time in terms of resource allocation, TSA is proposing the physical screening of vendor employees working in sterile areas as part of new measures to tighten access to sterile and SIDA areas. The TSA proposal requires that airport operators:

1. Require all vendor employees (concessionaires) who work in the sterile area of an airport to access the sterile area through the TSA screening checkpoint and receive physical screening;

2. Reduce the number of operational doors that lead from a public area of an airport to a sterile area of an airport and include new enhanced security measures (eg. closed circuit television, contract security guards, etc.) at the remaining operational doors; and

3. Limit the number of vendor employees working in the sterile area who have unescorted access to the SIDA.

Furthermore, TSA also believes in enhancing security measures currently in place in order to strengthen the physical security of restricted areas at airports. TSA is considering new security measures, such as a reduction in the number of pedestrian and vehicle access points; an increased number of random security patrols; additional random identification checks of persons and vehicles entering the secured areas and SIDAs from

public areas; additional random identification checks of persons entering the sterile area from the SIDA and entering the SIDA from the sterile area; and enhanced response procedures for when the alarm on a door to the SIDA sounds.

While none of these measures will provide a 100% security guarantee, they represent a significant set of mutually reinforcing safeguards when taken as a whole, consistent with our layered security approach.

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

50. Please describe the timeline for the implementation for the TWIC program. When will it be implemented nationwide?

Answer: TWIC is well underway. Phase II, the technology evaluation phase, was completed October 2003. Following the TSA and DHS review of the results of Phase II, and after extensive consultation with Congress the decision was made to move forward with Phase III, the Prototype Phase.

The Request for Proposals (RFP) for Phase III was released on May 10, 2004. The Prototype Phase will test and evaluate an integrated identity management solution across all transportation modes. It includes 42 separate facilities in three regions: East (Philadelphia-Camden, NJ-Wilmington, DE), West (Long Beach-Los Angeles) and the state of Florida (14 deepwater ports). The Prototype Phase will start in the summer of 2004 and last approximately 7 months.

TSA will review the results of Prototype Phase and provide a recommendation to DHS with respect to nationwide implementation. DHS will then determine if, when, and how the TWIC should proceed to a full nationwide implementation.

51. What plans does TSA have to issue TWIC cards to foreign crews on ships?

Answer: The TWIC is intended for transportation workers who require unescorted access to secure areas of the transportation system. TWIC holders must be either U.S. citizens or have legal presence in the United States. During the Prototype Phase, TSA does not have plans to issue TWICs specifically to foreign crews on ships. Individual foreign crewmembers, whose specific duties require unescorted access to secure areas, and who otherwise meet the requirements, would be able to apply for a TWIC.

52. Please identify the primary challenges being faced by TSA in implementing the TWIC program.

Answer: TWIC is a complex project that needs to balance three key goals: improving security, enhancing commerce, and protecting personal privacy. Similar to other large integrated projects, TWIC has inherent management and technology challenges as well as program-specific challenges in the fields of identity management systems, information

technology, information security, advance credential technology, biometrics, encryption, and physical and logical access control technologies.

We feel our primary challenge is the need to meet our stakeholders' expectations for solutions to their security needs consistent with the exercise of commerce and the safeguard of privacy. The message from our stakeholders is clear—in general they strongly support the TWIC concept and have compelling security needs that TWIC helps satisfy.

53. An identity card, particularly one that grants access to sensitive and secure areas such as in airports and ports, is only effective if the issuing agency can be confident that the person receiving the card is who she or he claims to be. How will TSA verify the identity of those to whom it issues TWIC cards?

Answer: Identity verification represents the core operational capability of the TWIC Identity Management System. Our approach to verifying identities, which is based on lessons-learned in the Federal Government and commercial industry, will be tested -- and refined as appropriate -- during this year's Prototype Phase. It will involve at least four key areas.

The first component is that all TWIC applicants must have a sponsor. The employer will often be the sponsor. When an employer does not exist as in the case of independent truckers, the local facility must sponsor him/her.

The second component is the requirement for documents that help verify an individual's identity, commonly referred to as "breeder" documents (e.g., birth certificate, government-issued photo ID, driver's license, utility bill, etc).

The third component of identity verification is collection of finger-based biometric samples. This biometric collection has two distinct purposes during Prototype Phase. The first use is to facilitate a one-to-many (1:N) search against current cardholders. This search prevents a distinct person from enrolling multiple times using an alias or from fraudulently enrolling. The second use of the biometric collection is for identity verification via a one-to-one (1:1) match. Biometric templates will be securely stored on the TWIC. By matching the cardholders biometric sample with the templates stored on the TWIC, we have much greater assurance that the individual is the rightful holder and owner.

The fourth component is a name-based threat assessment. Once we have verified the identity of the applicant, the system will conduct a name-based threat assessment against known or suspected terrorists. Once we have the proper rules in place, we intend to conduct FBI background checks on all applicants in addition to the name-based threat assessment.

54. Only those who need to have access to secure areas of transportation facilities, such as in airports or ports, should be eligible to hold a valid TWIC card. For example, this means

that TWIC card holders must be currently employed in a position that requires such access. What steps will TSA put in place to ensure it has continually updated information on individuals who leave their employment or should be made ineligible for other reasons, such as conviction of a disqualifying crime? If a TWIC card holder changes jobs, and requires a different kind of access than he or she had previously, how will TSA obtain and maintain this information and make the appropriate adjustment in the card holder's access privileges?

Answer: Current and accurate information is at the heart of any IT system, and is a key operational capability of the TWIC identity management system. During this year's Prototype Phase, we will put our processes and procedures to the test to ensure that we have made the right considerations for maintaining current and accurate information on TWIC cardholders. Today, these considerations include the direct involvement of employers and sponsoring entities (i.e., facilities) and periodic checks to ensure that the cardholder remains qualified.

A key operational capability of the TWIC identity management system includes a centralized revocation and alerting capability. If a cardholder is made ineligible for a TWIC, the system would "hot-list" the unique card number and notify the local facilities where the individual was granted access. This action would result in preventing the individual's unique card number from being successfully used for access.

Local facilities are responsible for granting or denying access to their facilities, and managing their access control systems. The TWIC represents a risk mitigation tool for local facilities as a result of two key capabilities. First, local facilities will be able to verify the individual's identity via a one-to-one (person-to-card) biometrics match, and secondly, to check to ensure the person remains eligible for a TWIC and that the TWIC hasn't already been reported lost or stolen (i.e., hot-listed).

OTHER MODES OF TRANSPORTATION

55. The nation's transit agencies may be facing hundreds of millions of dollars or more in needed security upgrades. What role will TSA play in providing security for transit systems? What role will the Federal Transit Administration play? Will TSA provide any mandatory requirements for transit security? How will TSA ensure that transit security is coordinated with other forms of transportation security?

Answer: DHS, DOT, and other Federal agencies are working together to enhance rail and transit security in partnership with the public and private entities that own and operate the nation's rail and transit systems. TSA has a unique role in transit and rail security in that TSA is uniquely positioned to look at and coordinate security efforts across the totality of the intermodal passenger and supply chain. This responsibility must involve the coordination of appropriate Federal, State, tribal, local and private industry partners, many of whom have always been and continue to be in the business of providing security for their particular piece of the transportation puzzle. TSA's main charge, both under ATSA and now as part of the DHS family, is to coordinate these

efforts under the guidance of the Secretary and the Under Secretary for Border and Transportation Security, identifying gaps and working with appropriate partners to ensure that those security gaps are filled.

DHS has assigned TSA primary Sector Specific Responsibility (SSR) for the Transportation Sector as DHS implements Homeland Security Presidential Directive 7 (HSPD-7), which directs the establishment of "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." In accordance with DHS's HSPD-7 implementation plan, TSA is developing the Transportation Sector Specific Plan (SSP). A first draft of the SSP is due to DHS by early summer 2004 (at the same time SSPs from the other 12 sectors of critical infrastructure are also due). In developing the transportation SSP, TSA is working under BTS guidance and in partnership the U.S. Coast Guard and the Department of Transportation (DOT), including the Federal Transit Administration. The SSP will discuss how federal and private-sector stakeholders will communicate and work together; how important assets in the transportation sector will be identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured; and how R&D will be prioritized in the sector. In the Transportation Sector, the SSP will further these efforts currently underway and help ensure that they are systematic, complete, and consistent with the efforts in the other 12 sectors.

Specific to transit and passenger rail security, passenger rail companies, in coordination with TSA, have voluntarily implemented a number of robust security measures. On May 20, 2004 DHS issued Security Directives (SD) to ensure the best of these practices are implemented throughout the industry. The SDs, which are being administered by TSA, establish 16 mandatory protective measures for commuter and transit passenger rail, inter-city train, and regional services. To enforce the directives, in coordination with the rail operator, TSA will designate Security Partnership Teams comprised of representatives from DHS/TSA and DOT. Team visits will be prioritized based on criticality, threat, and the status of the last vulnerability assessment.

56. Describe TSA's plans to improve screening of rail passengers and baggage.

Answer: TSA is evaluating the efficacy of establishing standards for passenger screening in a rail environment. Towards that end, TSA implemented a pilot program in New Carrollton, Maryland, to test the feasibility of using emerging technologies for screening passengers and carry-on items for explosives at rail stations and aboard trains. This pilot, the Transit and Rail Inspection Pilot (TRIP), is being conducted in partnership with AMTRAK, MARC, Washington Metropolitan Area Transit Authority (WMATA), and DOT for a 30-day period. The TRIP pilot program does not resemble an aviation-type solution to transit and rail security challenges, but rather provides a venue to test new technologies and screening concepts to determine their effectiveness in the transit and rail environment. Rail stations are not self-contained, and passengers have the freedom to board and disembark trains throughout their routes. TSA intends that the TRIP program provide necessary data to determine if rail and transit operators might be

able to deploy targeted screening resources and protocols in high threat areas or where specific intelligence indicates there is a need. Additional phases of the pilot are under consideration.

57. Describe what you believe should be the division of responsibility between the Federal Railroad Administration, TSA, and IAIP in the assessment of vulnerabilities of the nation's railways. Describe what you believe should be the division of responsibility between the FTA, TSA and IAIP in the assessment of vulnerabilities of mass transit systems. Are these assessment processes working as you believe they should or do you think changes are necessary? Please explain.

Answer: TSA conducts criticality assessments using a criticality assessment tool that was built in conjunction with IAIP and is a derivative of the National Infrastructure Protection Center (NIPC) tool set from the FBI. Information on results is shared with IAIP and among Federal agencies, such as the FRA TSA is also working closely with FRA and FTA in the development of a mass transit and passenger rail self-assessment module for use in conducting vulnerability assessments. TSA is also working closely with IAIP on cargo rail assessments.

58. It is our understanding that TSA has not reviewed vulnerability assessments conducted by rail carriers and other relevant parties because of a concern that the vulnerability assessments would be subject to FOIA if TSA obtained them. Please explain the nature of these concerns, and explain what action is being taken to address these concerns.

Answer: TSA has never had a concern about the FOIA protected status of vulnerability assessments provided to TSA. All vulnerability assessments submitted to TSA as part of an examination of a transportation system, vehicle, or facility to determine its threat-based risk of unlawful interference are considered sensitive security information (SSI) and are exempt from FOIA. Some entities, however, have been unwilling to turn over security-related documents to TSA, citing their concerns over TSA's ability to exempt information from FOIA. Under rail security directives issued by DHS in May 2004, passenger rail owners and operators will be required to turn over certain TSA-requested information, including vulnerability assessments, if available. TSA is developing a regulation that would clarify this issue and protect sensitive security information in the non-aviation transportation sector.

59. Please describe your view of TSA's role and responsibility for security in each of the following modes of transportation:

a. passenger rail

b. freight rail

c. mass transit

d. pipelines

e. trucking

Responses to Questions 59a-e, appear in the consolidated answer below:

Answer (a. – e.): The nation's transportation system, as you know, is vast and complex, and very few of its assets are owned or controlled by the Federal Government. Only in aviation is the Federal jurisdiction truly exclusive. And for that reason, right from the very start, TSA and its parent department, DHS, have known that the aviation model would not work as well for securing all modes of transportation. Thus, we have worked with our State, tribal, local, regional and private partners to help secure our transportation system. These efforts span the spectrum of security, from intelligence and information sharing and awareness through prevention, response and recovery to a potential terrorist attack in the United States.

Under DHS leadership, TSA is responsible for 1) establishing consistent national transportation security standards across all modes, 2) monitoring compliance with these standards by transportation stakeholders, 3) evaluating risk to the system across a changing array of threats, 4) sharing threat and risk information with transportation stakeholders (public and private), and 5) in the event of a transportation security incident insuring rapid restoration of service and public confidence. TSA is currently engaged in this process through rulemaking, risk modeling and contingency planning. The challenge in implementing this strategy centers on the proper balance between public and private responsibility/investment in achieving an acceptable security level. TSA/DHS will work with transportation stakeholders (public and private) to develop consistent security standards across all transportation modes.

The success of transportation security rests on the close partnership between DHS and transportation stakeholders. While clearly private investment in security is expected, the threat-based risk-managed approach complemented by performance based standards – which permits achievement of security standards within an owner's business model – coupled with appropriate security grants mitigates the national cost borne by the private stakeholders. Aggressive inspection/auditing of compliance with national transportation security standards ensures acceptable risk to the national transportation security system.

DHS has assigned TSA primary Sector Specific Responsibility (SSR) for the Transportation Sector as DHS implements Homeland Security Presidential Directive 7 (HSPD-7), which directs the establishment of "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." In accordance with DHS's HSPD-7 implementation plan, TSA is developing the Transportation Sector Specific Plan (SSP). A first draft of the SSP is due to DHS by early summer 2004 (at the same time SSPs from the other 12 sectors of critical infrastructure are also due). In developing the transportation SSP, TSA is working under BTS guidance and with partners in the U.S. Coast Guard and the Department of Transportation (DOT). The SSP will discuss how

Federal and private-sector stakeholders will communicate and work together; how important assets in the transportation sector will be identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured; and how R&D will be prioritized in the sector. In the Transportation Sector, the SSP will further these efforts currently underway and help ensure that they are systematic, complete, and consistent with the efforts in the other 12 sectors.

60. Clearly defined missions, roles and responsibilities are critical to the successful and efficient implementation of security measures, and necessary to ensure that officials are accountable for carrying out their responsibilities. An effective national security system requires the cooperation and participation of several Federal departments and agencies. However, thus far, TSA has failed to enter into "memoranda of understanding" (MOUs) with relevant transportation agencies in order to clearly define their respective roles and responsibilities in ensuring transportation security.

a. What specific steps will you take to ensure that TSA has a Memorandum of Understanding with the Federal Transit Administration (FTA) and the Federal Railroad Administration (FRA)?

Answer: DHS and TSA work closely with the Federal Transit Administration and Federal Railroad Administration in safeguarding rail and transit security. The Department is pursuing channels other than entering into a formal memorandum of understanding (MOU) to facilitate this coordination. A mechanism for coordination exists through Homeland Security Presidential Directive-7 (HSPD-7), which "establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attack." The Secretary of the Department of Homeland Security, in accordance with paragraph 15 of HSPD-7, has the lead role in coordinating protection activities for "transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems." Pursuant to HSPD-7, the Department of Homeland Security and the Department of Transportation will "collaborate on all matters relating to transportation security and transportation infrastructure protection." (paragraph 22(h)). As discussed in more detail below, we believe at this point that the HSPD-7 process meets the coordination needs for DHS, DOT, and their respective component agencies.

b. In the absence of such MOUs, how will you ensure that the appropriate officials are held accountable for carrying out their responsibilities in assessing and addressing transportation security needs?

Answer: DHS has assigned TSA primary Sector Specific Responsibility (SSR) for the Transportation Sector as DHS implements HSPD-7. In accordance with DHS's HSPD-7 implementation plan, TSA is developing the Transportation Sector Specific Plan (SSP), due to DHS by early summer. In developing the Transportation SSP, TSA is working under DHS guidance and with partners in the U.S. Coast Guard and the Department of Transportation. The SSP will discuss how Federal and private sector stakeholders will communicate and work together; how important assets in the transportation sector will be

identified, assessed, and prioritized; how protective programs will be developed; how progress in reducing risk will be measured; and how R&D will be prioritized in the sector.

In the Transportation Sector, the SSP will further these efforts currently underway and help ensure that they are systematic, complete, and consistent with the efforts in the other 12 sectors. DHS will build on the foundation of the SSP to provide overall operational planning guidance on rail security. The expanded SSP will ensure that modal security plans are integrated into an effective concept of operations for management of security of that sector of transportation.

c. How will you establish goals and performance indicators for federal efforts in transit and rail security by multiple agencies so that security goals are met?

Answer: Through the National Infrastructure Protection Plan (NIPP) for the Transportation Sector, performance data and measures for all aspects of transportation security are being developed in conjunction with all relevant agencies and stakeholders. The focus on critical infrastructure protection (CIP) is still new, and this carries advantages and disadvantages. One advantage is the clean slate from which to develop effective processes, procedures, and practices. On the other hand, it will take a significant period of time to generate a statistically significant amount of data to support a rigorous analysis of performance, as determined by the impact (or outcome) of activities. Along the way, we must be vigilant about collecting the information that will enable thorough analyses in the future, and we must hold ourselves accountable through the use of milestones and output measures. Accordingly, the framework on which we will build our performance measures and measurement activities includes:

- Long-term performance goals, objectives and strategies
- Long-term performance measures (outcomes) to track performance toward defined goals
- Intermediate performance measures (outputs, also a type of "process metric")
- Milestones (one type of "process metric")
- Descriptive data (e.g., numbers of assets by type, percentage of an asset class owned by the private sector)

To ensure that the SSR defines the right long-term performance goals, and that we are able to collect data and report accurately on long-term performance, we need to direct our measures at our overarching goals, objectives, and strategies. In the case of critical transportation infrastructure protection, the SSR defines the overarching goals (as stated above) as:

- ***Awareness:*** Identify and assess the vulnerability of the nation's critical transportation infrastructure/key transportation resources;
- ***Protection:*** Ensure protection from terrorist attack for the nation's critical transportation infrastructure/key transportation resources;

- ***Partnership:*** Establish a collaborative environment across all levels of government and between the Government and the private sector to effectively protect the nation's critical transportation infrastructure/key transportation resources; and
- ***Coordination:*** Coordinate and integrate, as appropriate, with other federal emergency and preparedness activities, including the National Response Plan.
  The Transportation Sector's critical infrastructure protection activities will support the achievement of these goals. They will also be used to measure progress. Resources will be directed toward those activities that best support accomplishment of the goals, and activities that are not advancing goals will be redesigned or eliminated over time.

The SSR's two primary objectives for transportation infrastructure protection have been defined as:

1. To identify and assess the vulnerability of—and to mitigate risk of terrorist attack to—the nation's critical transportation infrastructure/key transportation resources, and
2. To mitigate any negative impacts of security activities on the public, relevant stakeholders, and the economy.

Four important strategies for achieving these objectives are:

1. Define a valid and consistent approach for identifying and assessing the vulnerabilities of critical transportation infrastructure/key transportation resources;
2. Establish a collaborative environment across all levels of government and between the government and private sector to effectively protect the nation's critical transportation infrastructure/key transportation resources; and
3. Coordinate and integrate, as appropriate, with other Federal emergency and preparedness activities, including the National Response Plan;
4. Define and execute a methodology for measuring the impact of transportation security activities on the public, relevant stakeholders, and the economy.
   An appropriate performance measurement framework for critical infrastructure protection then includes measures of performance in achieving each of these major objectives. In addition, it requires that sector personnel understand performance at the lowest levels (by asset) and that we are able to roll those data up until we reach the system level.

To understand performance at the lowest levels (by asset) and roll those data to the system level, we have to track performance against:

- Transportation Sector
- Transportation Mode (six)
- Transportation Entity (each major type of transportation entity—e.g., air cargo shippers, airports, general aviation—within each of the six modes)
- Transportation Category (e.g., cargo vessels, 500 tons, tank ships and bunkering vessels—within each major type of transportation entity within each of the six modes)

d. Do memoranda of understanding exist between TSA and agencies outside of the Department of Homeland Security regarding each agency's respective role for security of pipelines or trucking? If so, please specify which agencies. If a memorandum of understanding does not exist between TSA and any agency that you believe has responsibility for security in these transportation modes, please state which agency has the lead for that mode of transportation and how that lead role has been established.

Answer: TSA does not have MOU's as described in the question, other than with the FAA. TSA, under the guidance of BTS and the Department, has the lead role for security in the Transportation Sector as a whole, and for inter-modal issues. This role was established by the ATSA, and by the Department's designation of TSA to lead the development of the Transportation Sector Specific Plan as part of the implementation of Homeland Security Presidential Directive 7 (HSPD-7).

Within the Transportation Sector, TSA has the lead for modal security in 5 modes: Aviation, Mass Transit, Rail, Highway, and Pipelines. The Coast Guard has the lead for maritime security within the Transportation Sector. TSA's lead in the Aviation mode was established by extensive Congressional direction in the ATSA and other legislation, as well as through Departmental directives.

In the Mass Transit, Rail, Highway, and Pipeline modes, TSA's lead is established by a combination of the ATSA; direction in HSPD-7 and the Department's implementation plan; the Coast Guard's lead is based on an its historical mission; legislation including the Homeland Security Act and the Maritime Transportation Security Act; and direction from the Secretary of DHS and the Undersecretary of BTS. This is well established in delegations from the Secretary.

61. What do you think is the appropriate role for private sector non-aviation transportation operators to play in deciding what security measures are needed for their operations and in paying for those measures?

Answer: The responsibility of securing our Nation's rail, ports, and other non-aviation systems is a shared one. Hence, TSA has worked to develop effective partnerships with the appropriate Federal, State, tribal, local and private industry partners, many of whom have always been and continue to be in the business of providing security for their particular piece of the transportation sector. TSA's main charge, both under ATSA and as part of DHS, is to coordinate these efforts under the guidance of the Secretary and the Under Secretary for Border and Transportation Security, identifying gaps and working with appropriate partners to ensure that security gaps are filled.

TSA's efforts in non-aviation security over the past two years have focused on greater information sharing between industry and all levels of government, assessing vulnerabilities in non-aviation sectors to develop new security measures and plans, increasing training and public awareness campaigns, and providing greater assistance and funding for non-aviation security activities. With our government and private sector

partners, TSA will continue to leverage existing security initiatives; coordinate the development of national performance-based security standards and guidance; identify and take action as necessary to improve the security of passengers, cargo, conveyances, transportation facilities and infrastructures. TSA will work with its government and industry stakeholders to continue these efforts, establish best practices, develop security plans, assess security vulnerabilities, and identify needed security enhancements.

62. TSA announced grants totaling $115 million in May and November 2003 for mass transit security needs. According to the American Public Transit Association, only $35 million has actually been distributed to the transit agencies.

a. What steps will you take to facilitate the distribution of the remaining $80 million?

Answer: The Office of Domestic Preparedness (ODP) within DHS, and not TSA, administers the mass transit security grant program and made the announcement referred to in the question. TSA will work with SLGCP on these decisions.

b. What is your timetable for getting these funds to the transit agencies that have been named as recipients of these grants?

Answer: Please see the response immediately above.

63. Secretary Ridge recently proposed that responsibility for certain transportation security grants, such as those to mass transit and rail operators, would shift to the Office of State and Local Coordination and Preparedness (SLGCP).

a. What role do you believe TSA should play in the decision-making and oversight process for such grants?

Answer: All of TSA's transportation security grants officially moved to the Office of Domestic Preparedness (ODP) [ODP will soon merge with DHS's Office of State and Local Government Coordination and Preparedness (SLGCP)]. TSA will continue its involvement in the transportation security grant competitive selection process by working with SLGCP.

b. What steps will you take to ensure that such grants are based on appropriate needs and security plans?

Answer: As stated in (a.) above, TSA will continue to assist ODP/SLGCP, upon request, in developing eligibility criteria for all transportation security-related grants in addition to reviewing eligible applications and making final award recommendations.

c. The Department's FY2005 budget request does not seek any specific level of funding for mass transit or rail grants. Do you believe that there will be a need for additional grants for mass transit and rail in FY 2005? If so, what role do you expect to play in any decision to set aside funds for this purpose?

Answer: Improving security is a shared responsibility among the Federal Government, States, tribes, localities, and the private sector. Federal assistance plays an important role in protecting our Nation's critical infrastructure, but we need to be careful to not segment funds for specific, narrow purposes. The Federal Government has provided significant assistance to high-risk transit systems through the Urban Area Security Initiative of the Office of Domestic Preparedness and will continue to do so into the future. Funds provided to States under the State Homeland Security Grant Program have eligible uses that support these purposes as well. States have been encouraged to include transportation and other infrastructure in their homeland security plans. In addition, local public transportation systems can tap $4 billion in annual assistance provided through the Federal Transit Administration (FTA) for security needs if the public transportation systems believe expenditure for that purpose is warranted. Efforts should be funded through existing programs for State and local assistance where resources are allocated based on State plans and the most urgent needs across all infrastructure categories and purposes. Overall, additional Federal assistance for local public transportation systems must be weighed against other homeland security needs, especially given assistance that is already provided through base programs.

64. Many of the nation's transportation systems – mass transit and rail stations, tunnels and bridges, in particular – are old and badly in need of retrofitting (e.g. hardening of infrastructures, enhanced ventilation systems, etc.), detection devices, communications and surveillance equipment, and other security measures in order to help deter and mitigate catastrophes. However, to date, there has been little funding dedicated to meeting the capital needs of transportation systems outside of passenger aviation.

a. Do you think DHS should provide funds for capital improvements to non-aviation transportation systems?

Answer: Efforts should be funded through existing programs for State and local assistance where resources are allocated based on State plans and the most urgent needs across all infrastructure categories and purposes. For example, the FY 2004 Urban Area Security Initiative (UASI) Grant Program provides funding to identified mass transit authorities for the protection of critical infrastructure and emergency preparedness activities. Allowable costs for both the urban areas and the mass transit authorities comport with the FY 2004 Homeland Security Grant Program, and funding is expended based on the Urban Area Homeland Security Strategies and transit system assessments. New resources for public transportation must be weighed against other pressing needs to ensure we are optimizing the use of Federal resources to the highest risks and security needs as defined by States and in the national interest.

b. If not, how will TSA help address these transportation systems needs and identified security risks?

Answer: The responsibility of securing our nation's transportation systems is a shared one. DHS, DOT, and other Federal agencies are working together to enhance the security

of non-aviation transportation systems in partnership with the public and private entities that own and operate them. The DHS grant program for improving rail and transit security in urban areas has awarded or allocated over $115 million since May 2003 for transit security, and makes available over $1 billion annually for states to allocate to homeland security needs based on state priorities, developed in coordination with the Department of Homeland Security, regions and localities. Eligibility for these grants includes equipment, training, planning and exercises. The Federal government has provided over $500 million in port security grant funds and $75 million in funding for the Operation Safe Commerce program to provide increased security at our ports and in the maritime cargo supply chain. Additionally, the Administration has requested $24 million for TSA to advance security efforts in the maritime and surface transportation arenas, and has requested that $37 million of the Federal Transit Administrations Urban Security Bus grants be available for security related projects.

In addition, DHS will continue to conduct the following activities and initiatives to strengthen security in surface modes:

- Implement a pilot program to test new technologies and screening concepts to evaluate the feasibility of screening luggage and carry-on bags for explosives at rail stations and aboard trains;

- Develop and implement a mass transit vulnerability self-assessment tool;

- Continue the distribution of public security awareness material (i.e., tip cards, pamphlets, and posters) for motorcoach, school bus, passenger rail, and commuter rail employees;

- Increase passenger, rail employee, and local law enforcement awareness through public awareness campaigns and security personnel training;

- Ensure compliance with safety and security standards for commuter and rail lines and better help identify gaps in the security system in coordination with DOT, with additional technical assistance and training provided by TSA;

- Continue to work with industry and state and local authorities to establish baseline security measures based on current industry best practices and with modal administrations within the DOT as well as governmental and industry stakeholders, to establish best practices, develop security plans, assess security vulnerabilities, and identify needed security enhancements;

- Conduct name-based terrorist focused background checks on all commercial drivers license holders endorsed to transport hazardous materials (HAZMAT), and put in place a process to conduct fingerprint-based background checks on a recurring basis for all 3.5 million HAZMAT truck drivers; and

- Study HAZMAT security threats and identify best practices for transport of HAZMAT.

65. On April 19, 2004, Secretary Ridge announced the formation of a federal task force to coordinate heightened security at upcoming special events. The task force will include DHS and nine other departments, as well as hundreds of state and local agencies, to coordinate security measures.

a. Can you describe what TSA's role in this effort will be and how you will ensure a greater focus on security for transportation systems during these events?

Answer: Although the United States Secret Service (USSS) has the lead, TSA has been a full participant in all National Special Security Event (NSSE) planning. There are six transportation related (modal) sub-groups involved in the planning for the NSSEs, and TSA is actively participating in all six. For the NSSEs, TSA will stand up an incident management group at the Transportation Security Operations Center (TSOC), and we will also provide 24-7 coverage at the local operations centers. For example, for the G-8 conference, TSA provided staff for five operations centers that were stood up locally. TSA also provides screener support to USSS, whereby TSA screeners work side by side uniform division USSS officers to conduct baggage and personnel screening to participants at event venues. For the G-8, TSA provided TSA screeners at five different venues throughout Savannah, St. Simons' Island and Sea Isle, GA. TSA also has helped to develop temporary flight restrictions and flight waivers for the events, as well as helping to coordinate commercial truck and highway security procedures for entry onto the venues sites.

b. Do you feel that increased funding for transportation security will be critical to the success of this task force? If not, why not and how will goals be met?

Answer: As Secretary Ridge announced, the country is entering a period in which there are several high profile events that the Department of Homeland Security believes could be attractive targets for terrorists. Across the country, there will be an increase in security – from a more pronounced local law enforcement presence to extra Homeland Security assets deployed during special events. Certain events designated as National Special Security Events (NSSEs) - the G-8 Sea Island Summit, Democratic National Convention and the Republican National Convention - will receive additional assistance from both the Federal government and state and local authorities. The G-8 Summit, which took place in Georgia from June 8-10, is an illustrative example of how the many agencies of DHS work together with the relevant local authorities toward the common goal of homeland security. Homeland Security agencies, including the TSA, USSS, USCG and others are equipped to provide security at our nation's most visible events in coordination with relevant local authorities.

66. In March, 2004, following the Madrid rail bombing, DHS announced several new Rail and Transit Security Initiatives, including the development of a rapid deployment Mass Transit K-9 program, which will include seven K-9 teams.

a. Given the fact that transit systems alone cover thousands of miles, with hundreds of access points, how will seven teams cover this extensive system?

Answer: This program would supplement existing K-9 efforts. Many transit agencies in the United States are already utilizing K-9 teams. The following transit agencies currently have their own proprietary canine resources: MTA New York City, Massachusetts Bay Transportation Authority (MBTA), Washington Metropolitan Area Transit Authority (WMATA), MTA Los Angeles, Bay Area Rapid Transit (BART), South Eastern Pennsylvania Transportation Authority (SEPTA), New Jersey Transit, Amtrak, Metropolitan Atlanta Rapid Transit Authority (MARTA), Chicago Transit Authority (Private Contractor), MTA – Staten Island Railway, Port Authority – Trans Hudson, Niagara Frontier Transit Authority, Tri-County Metro Transportation District, and Metropolitan Transit Authority of Harris County. All other transit agencies operate in cooperation with local, State or Federal law enforcement resources.

TSA has 300 K-9 teams deployed at 64 airports nationwide. Currently, approximately 3 percent of their time is being used to support mass transit in places where mass transit connects to the airport. Phase I of the Department's Mass Transit K-9 program includes utilizing existing Homeland Security explosive K-9 resources. These mobile DHS response teams will be prepared to assist local law enforcement teams during higher threat periods.

In a related effort, DHS IAIP is cataloging federal, state and local K-9 resources across the country, which will facilitate rapid deployment in case of heightened need in a particular area.

b. Do you plan to expand this initiative and/or train localities to develop their own K-9 teams? If so, what is your timetable for doing so and what resources will TSA need to accomplish your goals?

Answer: Please see the response immediately above (66.a.).

67. Many experts believe that public education and awareness will be critical to any mass transit security plan. They highlight the knowledge and participation of citizens in London as an example of an engaged public. What plans do you have for a public awareness campaign in U.S. mass transit systems? How will you work with localities to develop education campaigns?

Answer: Public outreach and education is a key component to safeguarding security in transit and other modes. To ensure ongoing communication with mass transit passengers and employees, TSA has partnered with the Federal Transit Administration on its Transit Watch Program, a nationwide security awareness program. Similar to the successful nationwide Neighborhood Watch crime prevention program implemented in the early 1970s, Transit Watch is intended to raise awareness of transit employees, riders and the

general public and is designed for easy and low-cost implementation. Transit Watch media kits have been sent to all State DOTs and FTA grantees (over 500 agencies).

TSA and FTA are working on an interagency agreement to address the distribution of additional funds that would assess the current Transit Watch Program and aid in the implementation or enhancement of the Program (including the printing of materials). TSA plans to use approximately $500,000 to ensure that the nation's highest risk transit agencies have implemented the Transit Watch Program or a similar passenger awareness program.

68. Thus far, TSA has invested considerable resources and attention to aviation security strategies. Relatively little time and funding has been devoted to protecting other modes of transportation, such as transit and passenger rail. At the same time, security experts warn that as we expand and enhance the security presence in one mode of transportation, terrorists will look to easier targets in other modes. In its 2002 report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, the National Research Council called for "layered security systems" that are specially designed to address the respective needs of different transportation systems. Unlike airports, transit systems are open systems with multiple points of access that are designed to provide maximum convenience in meeting daily transportation needs.

a. Given the vast difference between the nature of air travel and other modes such as transit, how will you ensure that other modes have comprehensive, layered security systems that include deterrence, mitigation, response and recovery measures that dissuade terrorists and protect travelers?

Answer: Please see the response immediately below (68.b.).

b. How would such systems be structured under your direction?

Answer: At TSA, we agree with the need for a layered approach to transportation security in non-aviation as well as aviation modes. Under the leadership of DHS, we are designing a security strategy for a broader spectrum of responsibilities than were present in the pre-9/11 world, ranging from enhanced awareness, intelligence and information sharing through prevention, protection, response, consequence management, and recovery.

The creation of DHS has produced a force multiplier and a vast network for awareness and information sharing to protect our Nation. Working under the guidance of the Border and Transportation Security Directorate (BTS), we collaborate extensively with other BTS agencies and with other DHS components, such as the Information Analysis and Infrastructure Protection Directorate (IAIP), and the U.S. Coast Guard (USCG), identifying opportunities to share information, resources, and expertise. We also continue to work closely with the Department of Transportation (DOT) and the modal administrations. They provide another vital link with transportation providers, and we

communicate daily to share expertise and to ensure that we make the best use of each organization's resources and opportunities.

TSA continues to work to improve coordination with our sister agencies within DHS, as well as with our other Federal partners. In this regard, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7) on December 17, 2003, which directs the establishment of "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." HSPD-7 sets the framework for DHS to develop a National Critical Infrastructure Protection Plan, and TSA has been specifically delegated the responsibility to develop the Sector Specific Plan (SSP) for Transportation under the National plan. The development of this plan will involve intensive interaction with other DHS directorates and agencies, such as IAIP and CG, in addition to DOT. The plan, which is currently being developed will: (1) identify participants in the sector, their roles and relationships, and their means of communication; (2) identify assets in the sector; (3) assess vulnerabilities and prioritize assets in the sector; (4) identify protective programs; (5) measure performance; and (6) prioritize research and development.

Working with our partners, TSA plays an active role throughout the entire transportation system providing research and development, advisory and direct services, and intermodal coordination. To ensure security in each mode of transportation at an operational level, TSA is also working with our Federal and other partners on the development of Modal Security Plans for each mode of transportation. On behalf of DHS and in conjunction with other Federal agencies, the completed Transportation SSP will guide and integrate a family of transportation modal security plans to prevent, mitigate, and respond to intentional disruption of the Nation's transportation systems while ensuring freedom of movement for people and commerce.

69. Security expert Jack Riley, Director of Public Safety and Justice for the RAND Corporation, has expressed concern that buses are a primary security vulnerability because they can be easily hijacked and can be driven close to other terrorist targets. What steps (1) has TSA taken and (2) does it plan to take to assess and address security risks related to buses?

Answer: The Federal Motor Carrier Safety Administration (FMCSA) commissioned a study for the US Motorcoach Industry in 2002 that identified the level of current and emerging security threats in the motorcoach industry. The study, conducted by the John Volpe National Transportation Systems Center, offered several "areas of opportunity" to enhance security including enhanced employee training and public outreach.

TSA has analyzed these threats and recognizes the security vulnerability that motorcoaches represent. We have maintained aggressive and regular outreach to motorcoach industry stakeholders both through in-person outreach at industry conferences and seminars and broader telephone discussions. Through the bus grants, TSA sponsored a massive train-the-trainer security workshop jointly developed by American Bus Association/United Motorcoach Association called Operation Secure

Transport. ABA/UMA has offered this security training at no cost to the industry at ten cities across the country and continues to mail copies of the CD to motorcoach companies.

Improved communication and intelligence sharing allows us to collect, evaluate and disseminate information to industry on security incidents through the Transportation Security Operations Center (TSOC). TSA is a member of the Bus Industry Safety Council and the Commercial Vehicle Safety Alliance – these safety groups have taken on a security role for the industry. TSA works with the industry including trade associations to share best practices and ideas for security enhancements.

We are working to migrate the application of the TSA Self Assessment Risk Model (TSARM) tool to the motorcoach industry. The tool has been used extensively in the maritime sector to conduct security assessments in compliance with requirements of the Maritime Transportation Security Act. It is expected that the tool would be used initially to address the larger motorcoach operations and would ultimately be leveraged to address smaller operations.

Additionally, we have developed security awareness pamphlets and bus driver tip cards that have been widely distributed to the motorcoach industry. The pamphlets and tip cards provide information to motorcoach drivers on what to do in the event of a security incident as well as what to look for to prevent an incident from happening, stressing the importance of reporting anything that appears suspicious or wrong. More than 220,000 brochures and tip cards have been distributed to the motorcoach industry since October 2003. In addition to security awareness training, the bus grants have funded bus driver shields and GPS tracking to allow for better monitoring of motorcoach assets.

70. Earlier this month, TSA began a month-long pilot project at the New Carrollton, Md. rail station, screening Amtrak and commuter rail passengers and their bags with explosives-detection devices. What information have you learned so far from this pilot regarding the feasibility and effectiveness of screening procedures for rail? Based on preliminary findings, do you foresee expansion of the program to other stations? What responses have you received to date from passengers using the New Carrollton station regarding the screening process and its impact on their commute?

Answer: The Transit and Rail Inspection Pilot (TRIP) at New Carrollton, MD conducted during May 2004, provided TSA with useful results and positive passenger feedback. The overall results of the pilot indicate adequate checkpoint throughput with minimal customer inconvenience. During the New Carrollton phase of TRIP, 8835 passengers and 9875 pieces of baggage were screened. Over 95% of passengers wanting access to the boarding platforms were screened, where the cycle time for one passenger through the process averaged just over 1.5 minutes, and the average "wait time" for passengers was 3.5 minutes. If passenger behavior changed to arrive 3-5 minutes earlier for train departures, all passengers and carry-on items could have been screened prior to trains departing.

All of the screening equipment performed satisfactorily in the open-air environment of the New Carrollton station. Filters indicated a higher level of contamination than experienced in the relatively controlled airport environment. Accelerated maintenance resolved the contamination issues. The TRIP pilot provided equipment manufacturers an opportunity to adjust maintenance protocols and procedures for an open-air environment. Seismic results of passing trains had no discernable effect. Environmental data (temperature, humidity, etc.) was collected and is being analyzed. TSA's Internal Affairs inspectors also challenged the pilot program. I will be pleased to provide the results of their covert testing in a closed setting.

The purpose of this pilot was to test equipment in the open environment of a rail station and see if it is feasible as a response option for mitigating a high threat situation. The preliminary findings from this pilot suggest that this system could be implemented if threats were made against a specific station, or in preparation for a special event (e.g. the national conventions of the political parties, major athletic events).

I am pleased to report that passengers were overwhelmingly receptive to the screening process during the New Carrollton phase of TRIP.

GAO ACCESS TO INFORMATION

71. In certain cases, the actions of TSA to protect vital transportation modes and services are considered sensitive and not for public knowledge. Yet, as a federal government activity, the actions of TSA must still be subject to scrutiny. One method this occurs through is the reviews and reports that the Congress tasks the General Accounting Office to perform on its behalf. We understand that GAO has experienced some difficulty in obtaining timely access to information it believes to be integral to its efforts to conduct its review of TSA programs, but that TSA and GAO are working to improve this.

    a. Are you aware of this situation, and what are you doing to provide GAO access to key data?

Answer: Yes, I am aware of GAO concerns regarding DHS responses to GAO requests for documentation, and I am committed, along with senior DHS leadership, to support the GAO process at DHS. DHS is committed to the routine of senior level GAO and DHS meetings to discuss the relationship and process issues and to identify and resolve emerging issues and trends before they become problematic. DHS Deputy Secretary Jim Loy and GAO Chief Operating Officer Gene Dodaro exchanged letters on this issue last February. Deputy Secretary Loy has pledged to conduct a thorough review of DHS internal processes to look for ways to streamline or optimize efficiency and further enhance timeliness.

In slightly less than 12 months, DHS has been presented with about 250 new GAO engagements, and is being tasked to address with action plans and documentation for more than 350 open GAO recommendations. Excluding ongoing briefings and document requests, this volume loosely translates to 5,000 DHS work-hours for just entrance and

exit conferences with GAO personnel. Currently, TSA is working with GAO on 39 TSA-related audits and tracking 19 open recommendations. Additionally, senior program, counsel, and management personnel have devoted countless hours briefing GAO staff and responding to GAO inquiries and document requests (for many procedures that are still being designed) as timely as possible.

To facilitate this process within DHS, shortly after standing up the Department on March 1, 2003, the DHS Chief of Staff and Acting General Counsel met with GAO's Managing Directors to establish ground rules for communication and document exchange. As a result, a comprehensive DHS / GAO Relations Management Directive was developed and put in place. Next, in record time, DHS designed and implemented a comprehensive GAO Tracking and Management System. This comprehensive system tracks and monitors all phases of each GAO engagement. This is a capability that GAO does not have and DHS has approached GAO to establish an electronic interface between the two agencies, which we believe will provide for more efficient and timely data exchange.

b. One concern we have heard is that TSA is not allowing access to "predecisional" data, often in cases when decisions have been finalized. What is your view on this issue, and what actions will you take to rectify this?

Answer: On occasion, DHS has encountered access issues with GAO regarding documents subject to Executive Privilege, but all have been resolved in a manner that enables GAO to complete its charge. Often, GAO audits address programs that are concurrently undergoing intensive TSA/DHS policy development and formulation, and GAO seeks responses and documentation for issues that have not yet been resolved within the Department or the Executive Branch. As a result, our ability to respond to these requests is contingent upon a critical judgment balancing responsiveness to GAO with safeguarding the Department's open, rigorous decision-making processes. Such deliberations are vital and must remain internal so that personnel can explore various options. TSA and DHS are working with GAO in these instances to identify alternative approaches or to otherwise resolve the issue in a mutually satisfactory manner. TSA will work closely with DHS in DHS' review of the Department's process to establish processes and procedures to facilitate GAO's audit process and to ensure that both GAO and DHS benefit from the GAO audit process.

TRAINING

72. The Homeland Security Act of 2002, Pub. L. 107-296, (HSA) and the FAA Reauthorization bill enacted in 2003 (Pub. L. 108-176) established a mandatory TSA-approved training program for flight and cabin crews to prepare them for potential hijack situations. The TSA, however, has yet to issue the minimum standard guidelines necessary to implement this program under the criteria required by these laws. Do you support the need to train flight attendants and cabin crew as envisioned by HSA and the FAA reauthorization bill? What steps is the TSA taking to issue these guidelines, and

when do you expect to fully implement the security training program mandated in HSA and the FAA Reauthorization bill?

Answer: The Vision 100 – Century of Aviation Reauthorization Act (FAA Reauthorization bill) contains two components related to crewmember self defense training.

(1) The first component relates to basic training programs that air carriers are required to develop and deliver to crewmembers.

Minimum standard guidance was provided to all air carriers following passage of the Aviation and Transportation Security Act to reflect changes to the Common Strategy. TSA intends to review this earlier guidance upon completion of changes to the Common Strategy, which is currently under revision and review within the Administration. We will develop and implement changes to the basic training guidance if any are identified as necessary during that review.

(2) The second component of Vision 100 requires TSA to develop and provide an advanced crewmember self-defense training program to flight and cabin crew volunteers. TSA has completed an Instructional Development Plan and is working to finish curriculum development in consultation with the Federal Air Marshals Service (FAMS), representatives of the air carriers and flight attendants, training and anti-terrorism specialists, and other subject matter experts. The planned curriculum includes many of the defensive tactics and other applicable components from the Federal Flight Deck Officer basic training course, and complements the "Basic" training program. The current program is envisioned as a 24-to 28- hour course with approximately one-third planned for classroom delivery and two-thirds presented as hands-on "mat room" training. TSA is exploring ways to deliver the training. Our plan is to conduct a prototype class with the final curriculum starting in August or September 2004, and to be ready for full implementation by December 12, 2004 as required by Vision 100.

73. The FAA reauthorization bill also directed TSA to "develop and provide" voluntary advanced self-defense training for flight attendants and cabin crew members. The FAA reauthorization bill became law on December 12, 2003, and requires that this training be provided no later than one year after that date, yet TSA's FY2005 Budget as presented to Congress in February 2005 does not request funding for this statutory obligation. Please explain why this program is not mentioned in TSA's Congressional Budget Justification. What are your plans for implementing this program on schedule as required by the FAA reauthorization bill?

Answer: Please see my response above (Question 72) for a discussion of advanced self-defense training for crew members. Regarding the FY 2005 budget, the TSA budget was completed by the time the Vision 100 Act was passed by the Congress and signed into law by the President. TSA is working within its resources to meet these requirements. We will continue to consult with Congress as this program develops.

HUMAN CAPITAL

74. The proposed regulations for the Department of Homeland Security's new personnel system under the Homeland Security Act would not apply to TSA employees. In testimony before subcommittees of the Senate Committee on Governmental Affairs and the House Committee on Government Reform, Comptroller General David M. Walker stated that DHS should consider moving all of its employees, including the more than 50,000 TSA screeners, under a single performance management system framework to help build a unified culture.

a. Do you believe that screener personnel and other TSA employees should be covered by the proposed new human resource management system? If so, what administrative, regulatory, or legislative steps would be necessary to accomplish such coverage?

Answer: In the creation of TSA, the Aviation and Transportation Security Act (ATSA) provided TSA with broad human resource management flexibilities under which they are currently operating, somewhat similar to those flexibilities provided in the DHS legislation. For this reason, TSA employees are not initially covered by the new DHS system. DHS is administratively extending the coverage to TSA employees other than screeners. In general, I am very pleased with the direction taken in the proposed regulations. I will continue with joint efforts to align TSA's personnel systems with the Department's system to the extent permitted by statute and consistent with the Department's goals. While pursuing this alignment, I believe that TSA should continue to exercise the broader personnel flexibilities provided by Congress in the ATSA.

b. If not, what steps will you take to help ensure TSA screeners and other employees are cohesive and effective components of DHS?

Answer: I believe our TSA workforce is already a cohesive and effective component of DHS. TSA's employees identify very strongly with the mission of ensuring homeland security. They stand up daily to the challenges associated with their extremely important jobs. Our screeners provide a human face to DHS with the public, interacting with almost 2 million airline passengers daily. One of my most important goals is to support the screener workforce in such a way that the screeners can concentrate on their immediate screening tasks without worry about organizational or administrative changes around them.

I believe there is an on-going job, however, of educating our employees fully about the other component agencies of DHS, what those organizations do, and how their own jobs may intersect with other organizations to provide comprehensive security coverage. If confirmed, I will continue to provide our employees with this needed information.

c. What due process rights and procedures do you believe should be made available to TSA screeners and other employees who believe they have been unfairly disciplined or have otherwise been subject to an inappropriate personnel decision? To what

extent do you believe due process rights and procedures currently in place are adequate, and to what extent do you believe changes are needed?

Answer: First, I would like to state that TSA screeners can join a union and be represented by a union for certain purposes. On January 8, 2003, acting under his authority under ATSA, Under Secretary Loy determined that screeners were not entitled to engage in collective bargaining or be represented by an organization or other representative in collective bargaining. TSA security screeners do have the right to join a union and have that union represent them *on an individual basis* in any matter where TSA Human Resource Policy authorizes an individual to have a representative. In addition, TSA employees may establish an allotment to a union or any other organization.

With respect to avenues of redress for screeners who believe they have been subjected to inappropriate or unfair personnel or management actions, TSA has established various programs and procedures. We have also created programs to allow employees to resolve issues informally and expeditiously.

- **Due Process**: Employees, including screeners, who have completed their probationary period, are entitled to due process for all adverse actions. This process includes advance written notice of the charges and the supporting documentation; an opportunity to reply, both orally and in writing; and a decision based on all the information stating the reasons for sustaining or not sustaining the proposed charges. Employees are entitled to representation during this process. If it is a first offense that does not require or necessitate removal, progressive discipline will, if possible, be employed. Non-probationary screeners have the right to appeal adverse actions to the Disciplinary Review Board.

- **Disciplinary Review Board:** The Disciplinary Review Board (DRB) provides non-probationary screeners with a forum to appeal adverse actions. The DRB consists of three management representatives who have no involvement in the action. The board reviews the matter based on the documents submitted and may also convene a conference with the appellant or conduct a hearing, which may include witnesses. The appellant has the right to representation in presenting an appeal to the DRB. The DRB has the authority to sustain the action, reverse the action, or mitigate the penalty.

- **Grievance Procedure**: All employees may file grievances concerning certain matters of dissatisfaction relating to their employment. TSA's process allows an employee who is dissatisfied with a decision at the first step to appeal to a higher level manager or supervisor who had no involvement with the matter. The decision of the second-step official is final.

- **Ombudsman Program:** This program assists employees in identifying and evaluating options for resolving specific concerns and problems using a variety of dispute resolution techniques. This is a confidential process that allows employees to

engage in a frank discussion with trained Ombudsman staff, with the assurance that the matter will not be relayed to management without the employee's consent.

- **Whistleblower Protections for TSA Screeners**: TSA prohibits retaliation against TSA screeners who engage in protected whistleblowing activity. Any screener who believes he or she has been retaliated against for protected whistleblowing activity may file a complaint with the Office of Special Counsel (OSC).

- **Model Workplace - Integrated Conflict Management System:** Through TSA's Model Workplace initiative, several pilot airports are participating in a program to implement local conflict management systems, including peer review. These systems are designed to provide screeners with a fair and expeditious process of redress for their concerns.

- **Equal Employment Opportunity (EEO) Process:** Any employee, including any screener, who believes that the agency has subjected them to prohibited discrimination by taking disciplinary or other action, based on their race, religion, gender, age, disability, color, national origin, or sexual orientation, may file an EEO complaint. If the matter is not resolved at the informal stage of the process, the complainant may file a formal complaint. If the issues are accepted, the complaint will be investigated and processed in accordance with EEO procedures. Employees may request a hearing before the EEOC, file appeals with the EEOC, and file actions related to their EEO claims in federal district court.

- **EEO Mediation Program – Alternative Resolutions to Conflict (ARC):** TSA's Office of Civil Rights has developed an aggressive program to resolve employee EEO concerns at the earliest stage of the process. ARC makes alternative dispute resolution available at both the informal and formal stages of the EEO process and offers an excellent opportunity for parties to work together to address their concerns quickly and informally without extensive administrative processing or the need for costly and time-consuming litigation. This program has the potential to dramatically reduce the number of formal EEO complaints, conserve limited resources, and restore trust in the employee/employer relationship. Employees have the opportunity to be represented during this process. Facilitations under this program are conducted by trained professionals and are scheduled expeditiously. Any agreements reached are binding on the parties. The Office of Civil Rights also arranges for facilitation or mediation in conflict situations that are not EEO-related.

d. What do you believe is the appropriate role of the TSA Office of the Ombudsman in addressing workplace complaints and issues involving TSA screeners and other employees? Do you believe the Office of the Ombudsman has adequate authority to assist TSA screeners and other employees with personnel matters?

Answer: I believe that the appropriate relationship between the TSA Office of the Ombudsman and the screening workforce is that the Ombudsman's office provides screeners with an independent, neutral, and confidential service. This service includes

providing the following to help TSA accomplish its mission: 1) furnishing clarification on policies, roles and responsibilities; 2) facilitating communication when employees or employees and managers are having trouble working together; 3) recommending cross-functional remedies if a generalized or systemic problem emerges; and 4) serving as an "early warning system" by identifying problems and conveying them to leadership in their early stages before they become acute. These activities are just a sampling of the myriad of services that characterize this relationship so that we may more effectively achieve our goals. So, when problems, issues, or conflicts arise, the TSA Office of the Ombudsman office can be called to investigate, mediate, and assist in resolving these matters impartially. In doing so, the Office of the Ombudsman is not an advocate for the employee, manager, or supervisor. More importantly, it is an advocate for fair programs and problem resolution by recommending and identifying solutions to ensure fair and equitable processes and procedures.

I absolutely believe that the TSA Office of the Ombudsman has adequate authority to assist TSA screeners with personnel matters. This authority stems from the fact that the Ombudsman's office reports directly to the Administrator through the Chief of Staff. They brief me regularly on key employee issues and concerns. They have my full support as advocates for problem resolution. To achieve this end, I expect every manager and supervisor to fully cooperate with Ombudsman staff. I have made it very clear to all TSA employees that the Ombudsman's office is responsible for providing assistance to all employees in resolving workplace issues. Any action meant to discourage an employee from seeking the Office of the Ombudsman's resolution services serves as a roadblock in developing a culture of constructive problem solving. I have also made it clear that I expect to be notified of any roadblocks and will ensure that those roadblocks are dealt with as appropriate. All TSA employees must be focused and vigilant in providing excellence in security and service - not distracted or disgruntled by workplace issues or problems that can be resolved through the ombudsman process. I will tolerate nothing less.

e. What steps will you take to address the continuing management challenges associated with establishing an effective personnel system for the screener workforce?

Answer: I am encouraging development in the following key areas:

(1) Employee Relations/Discipline Process: Utilizing our authorities under ATSA, we are developing an expedited employee relations/discipline process. The process will increase accountability of the supervisors while holding employees responsible for the results, using problem solving and the Integrated Conflict Management System from our Model Workplace initiative. The basis for the expedited process is fact-finding review and discussion that should take place within 3 days of an incident. The process is built on values that recognize the value of employees and ask managers and employees to exercise their rights while also solving the problem based on their best interests.

(2) Human Resources Management Program Guidance/Policy: TSA will continue to develop its own policy in several areas with a large impact on screeners. For example, we are developing policies to govern screener scheduling, an employee exit program, and reasonable accommodation. We are also working on a personnel interchange agreement that would facilitate movement of TSA employees to other positions both within the Department and to and from other agencies.

(3) Supervisor/Manager Training on Human Resources Management Issues: An effective personnel system requires that supervisors and managers know their responsibilities, flexibilities, and limitations within key human resources subjects. We are emphasizing training for supervisors and managers in Employee Relations, Workers' Compensation, the Employee Assistance Program, as well as for a Drug and Alcohol Free Workplace. These programs are particularly important for TSA because so many of our supervisors and managers did not come from other federal agencies or organizations where these or similar programs were utilized.

(4) Human Resources Management Technologies & Metrics: We have begun information technology initiatives to increase efficiency, moving towards paperless personnel action processing and electronic official personnel files. We are also working to use the human resources data we have available to drive progress focused on short and long range planning for human capital requirements.

(5) Retention of Part-Time Screeners: We are exploring options to encourage our part-time workforce to stay with TSA for longer periods of time. For example, we have a pilot program at Dulles Airport to subsidize parking, to give a retention bonus and to give referral bonuses. We are also looking into some flexible options regarding benefits.

75. On January 9, 2003**,** shortly before TSA was merged into the newly established DHS, the head of TSA issued an order prohibiting federal baggage and passenger screeners from unionizing. At the time, Admiral Loy explained in a statement: "Fighting terrorism demands a flexible workforce that can rapidly respond to threats.... That can mean changes in work assignments and other conditions of employment that are not compatible with the duty to bargain with labor unions." However, in enacting the Homeland Security Act, Congress established that collective bargaining would generally be allowed at DHS, and the proposed regulations for the Department include specific collective bargaining rights and procedures for the Department. These rights and procedures would apply to many DHS security personnel on the front-lines fighting terrorism, such as employees from the Customs Service, Border Patrol, Immigration and Naturalization Service, and the Animal and Plant Health Inspection Service, who have a long tradition of collective bargaining. Do you believe that the TSA baggage and passenger screeners should be allowed to engage in collective bargaining as are these other DHS security personnel? Please explain.

Answer: As I noted earlier (*see Question 74.c.*), on January 8, 2003 then Under Secretary Loy issued his determination that it was not compatible with TSA's security mission for TSA to engage in mandatory collective bargaining with airport security screeners. I support that decision, which was issued under the authority that Congress gave to TSA when it created the agency in the Aviation and Transportation Security Act. Given the continuing need to shift resources rapidly to meet changing threat conditions and surges in passenger loads, Federal Security Directors require maximum flexibility in managing their workforce. This requisite degree of flexibility is not possible if collective bargaining must occur before those management changes are implemented.

TSA has put in place a number of important programs to ensure that our airport screeners, and indeed all TSA employees, have effective mechanisms to ensure that their employment rights are protected. I have detailed some of those programs in my earlier responses. I have also clarified that TSA screeners may join a union for purposes other than engaging in collective bargaining and can be represented by a union on an individual basis in any matter where the employee is authorized to have a representative speak on their behalf. Additionally, we have an office within TSA devoted to developing and implementing a Model Workplace program at our airports. This program obviously includes screeners as a primary focus and provides mechanisms for conflict resolution.

76. In September 2003, GAO issued a report based on its preliminary review of airport passenger screening at the TSA (GAO-03-1173). While recognizing that TSA had taken steps to establish recurrent and supervisory training, GAO found that the training modules needed further development. The report also stated that, at the time, TSA collected little information regarding screener performance in detecting threat objects.

a. Do you believe that the current level of training for screener personnel is sufficient?

Answer: While we note that TSA has made significant progress over the past five months in improving the training available to screener personnel, additional work is required and is on going in this critical area. In April 2004, TSA completed a review of our original basic training courses with subject matter experts in screening operations, and introduced a new basic training curriculum that provides for basic training in both checkpoint and checked baggage disciplines. This new basic training course reflects one of three components in our overall training program for screener personnel. The second component is a recurrent training program that provides elaboration on topics initially introduced during basic training along with training products designed to sustain or improve critical screening skills. TSA has implemented 12 of 16 planned recurrent training products and is finishing development of the remaining 4 products. Training under the third program component, advanced training, started in May 2004 with the roll out of On Screen Alarm Resolution Protocol training for in-line Explosive Detection Systems (EDS) operators. Once these planned products are developed and delivered, we will assess their performance impact and identify additional training courses and products that will help improve operational performance.

On March 30, 2004 TSA completed basic leadership training for nearly 3,800 screener supervisors through the U.S. Department of Agriculture Graduate School. Further classes are scheduled for supervisors promoted or hired into these key front line positions since we started the training initiative in August 2003. In March 2004, TSA also implemented a basic screener supervisor technical course to provide supervisors and lead screeners with additional specific technical knowledge focused on resolving alarms and responding to other operational problems. TSA is currently assessing the supervisory training courses to identify additional technical training required by screener supervisors. We have also initiated a training needs analysis of the screener manager position to develop a leadership course specifically tailored to the needs of these managers. These training courses will ensure the Screener Supervisors, Lead Screeners and Assistant Federal Security Directors for Screening are provided with the correct tools to ensure the screening workforce is operating at maximum efficiency.

b. What revisions, if any, do you believe should be made to the screener training program?

Answer: Overall, I believe that the direction we have established for screener training over the past six to eight months is the correct approach. However, the training program for screener personnel requires frequent review to ensure that we are meeting the needs of our screener workforce as indicated by operational performance, and I am committed to this process.

c. If confirmed, what steps will you take to ensure an appropriate level of training is made available to TSA's current and future screener workforce?

Answer: I believe three steps are required to strengthen our training program for the screener workforce and if confirmed I will carry these out.

(1) We need to provide every airport with the capability to deliver screener training at the local airport level and move away from the centralized delivery model employed since airport federalization.

In my capacity as Acting Administrator, I recently directed the first step in this transition by initiating an effort to train screeners and Federal Security Director (FSD) staff to deliver new hire basic training for future screener workforce. TSA completed instructor training for over 650 FSD nominated employees on May 15, 2004. Additional instructor classes are being scheduled to accommodate FSD nominations received since April 1, 2004. We also restructured our Specialized Security Training Contract with Lockheed Martin to a supporting role for FSDs in conducting their own new screener training and cross training. Starting on June 1, 2004 the default approach to basic training for all new screener workforce will be to conduct this training locally with support from Lockheed Martin as required and requested by the FSD.

(2) We need to continue using a direct link between screener performance and our training programs through frequent analysis of operational performance data and the

development of targeted training products to address and resolve performance deficiencies.

Local covert testing by Federal Security Directors has been in place for the last month and data are being recorded in our Learning Management System (Online Learning Center). These results provide an additional measure of operational performance from which to discern targeted training interventions to improve overall performance.

(3) We must conduct a comprehensive review of the entire training program to ensure screener training is approached as a continuum in which the necessary content at the appropriate level of detail is provided throughout the screener's employment.

This effort requires the development of performance-based terminal training objectives for the overall training program with specific enabling objectives for all training and screener development products to ensure that every training opportunity is directly supporting screener performance.

In addition to these direct improvements to our training program for screeners, we must provide broadband connectivity to every checkpoint, screening lane, and training room. Direct access to training materials by the screening workforce in these locations is a key training enabler and allows the workforce to take advantage of operational lulls to complete recurrent and skills refresher training.

d. What is the status of the annual screener certification program?

Answer: TSA completed the first annual re-certification between October 17, 2003 and March 30, 2004 for all federal and contract screeners hired prior to July 30, 2003. To be re-certified, screeners had to pass all applicable modules of the Knowledge and Skills Assessment Program and have a rating of 'meets or exceeds' standards on their FY 2003 Personal Performance Assessment. Overall, less than 1% of screeners failed to re-certify. As of May 2004, over 42,000 screeners completed their annual re-certification. Screeners were afforded one opportunity for remediation and retest and those who did not re-certify were terminated.

77. In February 2004, the DHS Inspector General released a report, "A Review of Background Checks for Federal Passenger and Baggage Screeners at Airports." The report discussed TSA's efforts to conduct background checks on its screener workforce. The IG noted that even with contractor support, TSA was not able to manage the background checks in an orderly and consistent manner. The report provided 12 recommendations for strengthening TSA's process for conducting screener background checks.

a. Do you agree with the 12 recommendations contained in the report?

Answer: TSA, through its Credentialing Program Office (CPO), is addressing or has already addressed the issues raised in the OIG Audit of Background Checks for Screeners (*A Review of Background Checks for Federal Passenger and Baggage Screeners at*

Airports, OIG-04-08). Substantial improvements have already been made and continued progress is forthcoming.

TSA has acted aggressively to implement OIG's 12 recommendations with the exception of recommendation 2, which recommends that TSA "complete the comparison study of the effectiveness of the Office of Personnel Management (OPM) and private sector background checks". OIG has been apprised that recommendation 2 will not be executed since the private sector and OPM background checks are used by TSA for complementary rather than competing reasons. While criminal and credit history are checked in both investigations, the pre-employment check takes 2-3 weeks to execute and is needed to ensure security BEFORE an individual is hired as a screener. The post-employment OPM Access National Agency Check and Inquiries (ANACI) investigation takes several months to execute and is a more in-depth review of an individual's background. This combination allows TSA to quickly assess an individual's security risk prior to employment, and then to review the most recent data as part of the OPM ANACI while the employee is still probationary. This process meets all security and Executive Order requirements, meets the time requirements necessary to keep the screener workforce properly staffed, and is cost effective. Based on the above, TSA has recommended to the DHS OIG that recommendation 2 be closed.

TSA has acted aggressively to close the other 11 recommendations and has recommended to OIG that 9 of these be closed as completed. Highlights of the 9 recommendations identified for closure are as follows:

- Screener position risk designations have been completed by a cross-functional team consisting of members from Aviation Operations, Human Resources and the CPO using the methodology in OPM's Suitability Processing Handbook. Based on this analysis, these positions are recommended for classification as Low Risk with a minimum investigation of a NACI; the conduct of an OPM ANACI meets this background check requirement.

- Processes are in place to ensure that all screener candidates are subject to a fingerprint based criminal history check that is successfully adjudicated BEFORE they are hired. In addition, prior to hiring, all screener candidates undergo a commercially conducted pre-screen investigation (described above) that checks criminal history, credit history and a risk assessment against terrorist databases. After hiring, all new screeners undergo an OPM ANACI to ensure compliance with EO 10450.

- A personnel security tracking system has been created, the Background Investigation Tracking System II (BITS II). This database now holds the results of each screener's fingerprint check, pre-screen investigation, the status of their ANACI and a significant amount of other information. BITS II provides insight into the CPO's workload and backlog through a series of routine reports. Drill down capability is also available to investigate areas of interest.

TSA has plans in place to close the 2 recommendations that currently remain open. Recommendation #8 requires tailoring of DHS's draft Interim Personnel Security Directive for TSA; this tailoring will be completed by July 1, 2004. Recommendation #9 requires documentation of CPO's workload with a subsequent hiring plan. We are moving aggressively to obtain a contractor-prepared staffing study for CPO's Personnel Security function, and estimate that such a study will be completed by August 1, 2004.

b. If confirmed, what steps will you take to ensure corrective action is taken?

Answer: I am committed to executing the actions that will allow me to recommend closing these remaining 2 audit items, and I obtain periodic updates to monitor progress. If confirmed, and I find that progress begins to slip, I will apply additional resources and/or management oversight to ensure timely execution.

78. TSA officials have acknowledged that the agency faces a high number of EEO discrimination complaints from airport screeners, warranting an overhaul of management practices, and the agency's Civil Rights Office faces a significant backlog of discrimination complaints. (See "Airport Screener Discrimination complaints Overwhelm TSA," *GovExec.com* (Jan. 23, 2004).)

a. What do you believe is the cause of the high number of EEO complaints filed against TSA? What training or other initiatives do you believe are needed to address this problem?

Answer: While TSA must remain sensitive to any allegations of discrimination, the number of complaints is not disproportionate given the stand-up of a 50,000 screener workforce and its subsequent restructuring in less than two years. In its first year, TSA fulfilled the Congressional mandate to conduct the largest Federal agency build-up in over 50 years. Implementing this requirement involved hiring of over 50,000 individuals at hundreds of duty locations nationwide and ensuring proper training. It also required TSA to concurrently build the infrastructure to provide employee support for that large workforce. In the following year, TSA received and met another Congressional mandate to eliminate 6,000 employees in a matter of months. As one might suspect given these events, the majority of complaints are from non-selected applicants and terminated employees. With the stabilization of the workforce, new EEO complaints are declining to levels comparable with other Federal agencies.

Specifically,

- The traditional employee support infrastructure was not in place. TSA employee support offices had to be built from scratch, including the Office of Civil Rights, Training, and Human Resources.

- A majority of complaints are from non-selected applicants and terminated employees. However, as this number declines, a larger percentage of new complaints will likely be for non-sexual harassment. This is in line with statistics

applicable to all Federal agencies, as reported by the U.S. Equal Employment Opportunity Commission.

- In FY 2002, TSA's start-up year, 634 EEO complaints were filed. Of those, 305 (or 48 percent) alleged appointment/hiring as the issue, and 195 (or 32 percent) alleged termination as the issue. As such, 500 (or 80 percent) of the EEO complaints filed were from persons who either failed to get jobs or whose jobs were terminated.

- In FY 2003, a total of 1,851 complaints were filed. Of those, 857 (or 46%) related to appointment/hiring or termination. The bulk of the termination-related complaints occurred between May and September when TSA was downsizing its work force per congressional direction to increase efficiency and effectiveness.

- In the first quarter of FY 2004, 446 complaints were filed. Of those, 124 (or 27 percent) alleged termination as the issue and 16 (or 3.6 percent) alleged appointment/hiring as the issue, for a total of 140 (or 31 percent) relating to either appointment/hiring or termination

TSA is working hard to ensure proper working conditions, training and advancement opportunities for its screeners and to reduce workplace conflict.

These efforts include:

- The Model Workplace Program Office - Integrated Conflict Management System (ICMS), which will provide all TSA employees and managers with skills and tools for addressing and managing conflict, and working cooperatively to solve problems and issues that arise.

- TSA's Office of Workforce Performance and Training (WPT) is partnering with OCR to develop and deliver effective training programs for managers, supervisors, screeners and other employees throughout the country in fiscal year 2004, including:

- Web-based training, classroom training, train-the-trainer initiatives, and training programs sponsored by other Federal agencies, such as the Community Relations Service of the Department of Justice.

- Recognizing the need to provide our front line supervisors with the tools they need to manage effectively the screener workforce, TSA has sent more than 3500 supervisors to introductory leadership training at the Graduate School, United States Department of Agriculture.

- Civil rights training for managers, supervisors and other trainers occurred at John F. Kennedy International Airport in February 2004; Seattle-Tacoma International Airport in March 2004; St. Louis International Airport in April 2004; and El Paso

International Airport in May 2004. Several other airports have requested and will receive civil rights training in 2004.

- The Office of Civil Rights provides four hours of Civil Rights related training during the initial orientation of new Federal Security Directors.

- The Human Resources Office began conducting supervisory leadership training (which includes Model Workplace and Civil Rights topics) at several locations throughout the country in February 2004.

In addition, TSA's Office of Civil Rights provides an alternative dispute resolution option to individuals who file EEO complaints. This process is known as ARC (Alternative Resolutions to Conflict). The Office of Civil Rights has developed an aggressive program to resolve employee EEO concerns at the earliest stage of the process. ARC makes alternative dispute resolution available at both the informal and formal stages of the EEO process and offers an excellent opportunity for parties to work together to address their concerns quickly and informally without extensive administrative processing or the need for costly and time-consuming litigation. This program has the potential to dramatically reduce the number of formal EEO complaints, conserve limited resources, and restore trust in the employee/employer relationship. Employees have the opportunity to be represented during this process. Trained professionals serve as facilitators and these sessions are scheduled expeditiously. Any agreements reached are binding on the parties.

b. What progress has been made in reducing any backlog of EEO complaints, and what do you believe should be done to improve the performance of the Office of Civil Rights in processing complaints?

Answer: Through the hard work and dedication of the staff in the Office of Civil Rights and its partners throughout the agency, TSA is proud to announce that the backlog of discrimination complaints has been eliminated. Steps to achieve this goal included:

Staff Changes

- Hired a new OCR Director in August 2003.
- Brought on nineteen additional staff members including a deputy director and three new managers, during September - December 2003.
- Contracted with Veteran Service Disabled Contractor to handle Formal Complaint Investigations.
- Detailed staff from other DHS components such as U.S. Customs and Border Protection, and other cabinet agencies like the Department of the Treasury.
- Developed law student intern program.
- Established new training program for staff to enhance skills and improve customer service.

Process Changes

- New procedures were implemented to resolve EEO complaints in their early stages. For example, a new conflict resolution program called Alternative Resolutions to Conflict (ARC), modeled after the successful Postal Service REDRESS Program, has been launched. The ARC program places employees who have filed an EEO complaint at mediation with a management official and a trained mediator. OCR is currently working to bring the parties together within a month of a complainant making a mediation request.
- Trained EEO specialists now staff the toll-free phone line to better address customer concerns.
- A customized database is being developed to improve tracking and case management

Results Already Evident:

- The EEO complaint backlog of complaints filed prior to December 2003 is gone
- The total number of EEO complaints filed per month has trended downward since January 2004, as have processing times. For example, in the first quarter of FY 2004, a total of 446 complaints were filed; in the second quarter of FY 2004, 212 complaints were filed.

Informal complaints are handled in a timeline consistent with the Equal Employment Opportunity Commission's regulations.

79. GAO reported earlier this year that TSA faces serious problems in hiring, deploying, and training its screener workforce. According to GAO, TSA faces a high attrition rate, and TSA's hiring process has hindered the ability of some of TSA's airport security directors to adequately staff passenger and baggage screening checkpoints without using additional measures, such as overtime. Screener shortages have also contributed to the inability to fully utilize Explosive Detection Systems and Explosive Trace Detection Systems to screen 100 percent of checked baggage for explosives by the congressionally mandated deadline of December 31, 2003 (GAO-04-592T, March 30, 2004, at pages 9-12). Do you agree with the concerns expressed by GAO, and, if so, how do you expect to address them?

Answer: TSA has acknowledged that improvements are needed in our hiring process, which was originally established on a centralized basis in order to meet the rapid growth required to implement the Congressional mandates for creating a Federal screener workforce during TSA's start-up period. Following that effort and subsequent restructuring, TSA's priorities are naturally shifting to meet the needs of a more stable workforce. Our system needs to adapt to allow airports to remain at their screening allocation and replace screeners leaving by attrition in a timely manner.

TSA is revamping the hiring process to allow for more localized control by FSDs to be able to hire screeners quickly. This new process is expected to reach some airports during

the summer in order to ensure TSA maintains a healthy force throughout the extremely busy months ahead.

TSA has had remarkable success at dramatically reducing pre-9/11 attrition rates. TSA is now averaging about a 15% annual attrition rate – although rates increased temporarily last year as a natural outcome of the reduction in force required to meet Congressionally mandated levels. Prior to federalization, screening companies reported rates as high as 100-200 percent in some instances. Nevertheless, TSA continues to examine attrition by individual airport and can take steps where necessary to correct any problems that may arise.

CONTRACT MANAGEMENT AND OVERSIGHT

80. In a January 2004 report, the DHS IG found that TSA contractors made final adjudication decisions on background checks for federal screeners; this practice contradicted the stated intent of the TSA Administrator, who told the IG that TSA intended to make final adjudication decisions while the contractors merely assisted in the process. The IG also found that TSA had not provided sufficient oversight of the contractors conducting the adjudications.

a. Is it appropriate for contractors to make final adjudication decisions on background checks? Please explain your answer.

Answer: Yes, it is appropriate for contractors to make some final adjudication decisions for background checks on TSA screeners. TSA's Office of Chief Counsel has determined that it is appropriate for contract adjudicators to make final "suitable" decisions but that Government approval, or final adjudication, is necessary for "unsuitable" decisions. All appeals of adverse adjudications are handled solely by Government personnel. This concept of operations allows TSA to operate with a lean Headquarters staff. TSA has a written Quality Assurance Plan that provides guidance on the oversight of contract adjudicator activity. Please also see my answer to "b." below.

b. Since the IG's report was issued, has TSA changed its practices with respect to contractors performing adjudications? If so, how?

Answer: Yes, in order to ensure the highest quality of contractor performance, TSA has developed effective procedures for oversight of contract adjudicators. These procedures entail specific qualification and approval of individual contractor adjudicators before they approve "suitable" decisions and a more robust quality assurance program to randomly review contractor adjudicator case files. These steps ensure the appropriate level of Government oversight of contract adjudicators.

81. In the January 2004 report, the DHS IG noted substantial contract management problems, and observed that "TSA senior managers and staff were consistent in their remarks that TSA has not effectively managed its contractors. Despite contract management weaknesses, TSA intends to continue to rely upon contract support rather than build an

infrastructure to replace functions currently performed by contractors." (Department of Homeland Security, Office of the Inspector General Report on Major Management Challenges, March 2004, page 47). The IG report comes after serious problems with an NCS Pearson contract for the hiring of screeners. That contract led to numerous allegations of waste and abuse, and costs that reportedly mushroomed from $104 million to roughly $700 million.

a. How do you intend to address contract management weaknesses at TSA?

Answer: TSA is committed to a high performing and cost-effective government. TSA's "corporate model" for major infrastructure functions and service activities is one of a program management/contract management function. TSA has taken steps within the context of our original model to enhance our contract oversight and management capabilities without resorting to a traditional Federal agency structure where infrastructure functions are provided only in-house.

With the enormous and unprecedented challenge of having to build a new Federal agency from scratch in a short time frame and with very few staff in place, TSA significantly used contracting services for certain activities, including human resources, information technology, training, financial functions, and call centers. As a result, the agency operates with a smaller Federal staff compared to other agencies of similar size, allowing us to focus on our core mission of providing transportation security.

This corporate model has served the agency well during the initial growth phases and we continue to use it. The outsourcing of activities enables work to be accomplished through a smaller number of Federal personnel that focus their attention on security performance and leadership. As a result, TSA personnel figures represent lean staffing today. Our experience demonstrates that the private sector contractors can be robust, flexible, responsive, and disperse human assets across the nation where TSA needs services to be provided.

Likewise, TSA has also learned from our early experience that there are risks with contracting out to such a large degree. Government must exercise proper controls through its program management/contract management office and must independently verify, through quality assurance teams, contractor performance. Our program management offices are staffed with Federal personnel who know and are held accountable for contractor performance metrics and cost controls.

TSA did initially face many challenges to meet the Congressional mandates to deploy a passenger and baggage security workforce and equipment nationwhile while concurrently building the infrastructure necessary to sustain operations. The agency recognized the need for considerable private sector assistance to meet the statutory deadlines. The basics of recruitment, assessment, in-processing, and training of people for the screening workforce were initially provided through two contracts. Lessons-learned from the initial effort to deploy the workforce resulted in separating these efforts in follow-on contracts that provide greater flexibilities both operationally and administratively. For example,

the initial contract for human resources services resulted in the realization that it would be better to address recruitment and assessment in one contract vehicle and all other services of in-processing and record maintenance in a separate vehicle.

Other lessons-learned from our early contract efforts also revealed the need for other actions and to initiate other practices, including:

- Development and implementation of a TSA Acquisition Model, approved by the Administrator in April 2003. As noted above, the Model includes accountable program managers for each program, addition of an acquisition policy and oversight role within the Office of Acquisition, and program governance by the senior leaders in TSA.

- Program reviews for each major program to provide periodic updates on the performance of each programmatic area. We look at performance, adherence to cost and schedule parameters, and support of the strategic plan in these program reviews.

- Formalization of our Investment Review Process consistent with guidance provided from DHS, and consisting of an Investment Review Board (IRB) composed of the most senior leaders and two subordinate councils to provide preliminary review and guidance for information technology (IT) and non-IT investments, respectively.

Also, TSA representatives continue to be intimately involved with DHS in developing its Acquisition Workforce Management Directive (MD). This MD will provide a career path for fourteen acquisition professional career fields, including program managers, contracting officers, quality assurance, and logistics personnel. The program is being designed for reciprocity with Department of Defense's program, and will address training, education, and experience requirements.

We are committed to developing, issuing, and conducting training on an acquisitions "field guide" to be used by TSA managers and their staff. We are also developing and instituting a Contracting Officer's Representative (COR) Certification Program. And, we are continuing to conduct workshops throughout Headquarters to assist program offices to improve their acquisition planning and execution.

b. Do you agree that building an infrastructure to replace functions currently performed by contractors is a legitimate response to TSA's contract management weaknesses? Please explain your answer.

Answer: Please see the response immediately above (81.a.).

82. In his answers to Senator Lieberman's post-hearing questions during the consideration of his nomination, Admiral Loy reported that "TSA employs the services of commercial

organizations in support of contract oversight and internal controls." Is there any downside to hiring contractors to oversee other contractors? Please explain your answer.

Answer: Where appropriate, TSA may employ an outside source such as a contractor to examine in whole or in part aspects of another contractor's performance to TSA. However, this practice has been done only on a selective basis. For example, we have employed contractors to conduct Independent Validation & Verification (IV&V) services for which TSA may not have staff with the requisite expertise and experience to assure thorough satisfaction of TSA requirements.

With regard to contract oversight, TSA has a contract management team on each of its major programs. Each team is responsible for all activities related to inspection of contractor's performance and documenting compliance/noncompliance with contract provisions, including cost/schedule performance. The contract management team is comprised of the Program Manager, Contracting Officer, Contracting Officer's Representative, Quality Assurance Specialist, and in some cases, other technical specialists drawn from outside sources.

Additionally, TSA has also drawn on the knowledge and expertise from non-TSA and non-DHS sources such the Defense Contract Audit Agency (DCAA) and Defense Contract Management Agency (DCMA) to support and strengthen all contract oversight functions. For example, the DCAA has performed over 130 individual contract audits on our behalf. In fact, TSA brought in DCAA very early to assist with its contract management and oversight.

"NO-FLY" LIST

83. What role do you think TSA should have in compiling, maintaining, and operating the "no-fly" list that is supposed to identify terrorists and other criminals and prohibit them from flying? Who has these responsibilities today? If you feel that TSA should have a greater role, how would you institute that change in how the "no-fly" list is handled?

Answer: At this time, the Transportation Security Administration compiles, maintains, and operates the No Fly list. TSA is partnered with the Terrorist Screening Center as all United States government watch lists are consolidated in accordance with Homeland Security Presidential Directive #6. TSA staff assigned to the TSC compile, maintain, and operate the list from the TSC facility to insure coordination with other government watch lists, and the accuracy of the Terrorist Screening Data Base (TSDB).

TSA has the responsibility for deciding whether an individual is placed on the No Fly List. This decision is based upon an analytic assessment of all watch list nomination data provided to the TSA. This decision-making process includes a review of the specific watch list request, the content and credibility of the threat information, and the completeness of the biographical data provided.

Based upon the quantum and gravity of information, the TSIS will consider for placement on the No Fly List those who present a significant:

- Threat to transportation or national security; or
- Threat of air piracy; or
- Threat to airline or passenger security; or
- Threat to civil aviation security; or
- Threat of terrorism because of known association with terrorists or involvement with terrorist groups.

A passenger who is on the No Fly List, along with any traveling companions, personal belongings, and baggage, is not permitted to board commercial flights.

84. Should TSA decide which names are to be placed on the list? Which agencies do you believe should propose name designations?

Answer: Yes, TSA is responsible and should retain responsibility for vetting nominations submitted for the No-Fly list. The process developed as part of Homeland Security Presidential Directive #6 is as follows. Federal agencies nominate foreign subjects for the TSA No-Fly List through the Terrorist Threat Integration Center (TTIC). Domestic nominations are submitted to the Federal Bureau of Investigation (FBI). These agencies review the submissions and forward them to the TSA representatives at the Terrorist Screening Center (TSC) for inclusion on the TSA Watch Lists. Time sensitive nominations may be submitted directly to the TSC if required.

BTS is currently leading a review of the No Fly list process, as well as how other information is used to make decisions about passenger screening by both CBP and TSA. This effort is fully coordinated with overall watch list consolidation and development of the TSC.

85. Do you think that all al-Qaeda terrorists who have been identified on any of our government's terrorist watch lists and who have received any kind of training in Afghanistan or elsewhere should be on the "no-fly" list? Do you know whether or not that is the current situation with the list?

Answer: Nominated Al-Qaeda and other terrorist group members who meet the criteria for the No-Fly List, have biographical data and unclassified information are placed on the list. As described earlier, nominations for inclusion on the list are received and reviewed by TSA representatives at the TSC; those individuals meeting the criteria are added to the list.

Currently in order to execute the checking of the No Fly list against international and domestic passengers the list is provided to foreign and domestic carriers. Therefore the list must be unclassified (Sensitive Security Information). As a result classified nominations are not part of the current list. Additionally, agencies are sensitive in their

nomination process to the risk of the list falling into the hands of terrorists as it is disseminated to foreign air carriers.

The Department of Homeland Security is currently looking at options to operate the No Fly list within the Government rather than within air carrier reservation systems. Under that construct the No Fly list could grow to include all terrorists known to the U.S. Government.

86. During a crisis period similar to the December 2003 to January 2004 holiday Orange Alert period, would you want passenger names on the manifests of foreign carriers leaving European capitals for the United States checked exclusively against the "no-fly" list or checked against all names on all of our terrorist watch lists? How would that be done?

Answer: Currently, I see the need for passenger manifests to be checked against all available watch lists in a heightened threat period or when there is a focused threat. However, as the Terrorist Screening Center and its Terrorist Screening Data Base become fully operational, all checks will be conducted at that single entry point.

87. What is your plan for a more effective and comprehensive "no-fly" list, what priority do you plan to give it, and how soon do you plan to implement it?

Answer: In the near future, all watch lists, including the No-Fly List, will become part of a Terrorist Screening Database (TSDB) at the Terrorist Screening Center (TSC). This centralization should help provide a more comprehensive list and "one-stop shopping" for agencies seeking information on terrorists who may be attempting to enter the U.S. The TSDB is scheduled to be on-line by the end of June 2004. Once activated, the TSC No-Fly list will be completely integrated into the TSDB. TSA will continue to have representatives at the TSC to assist in the vetting and adjudication of name nominations for the list. As part of this process, a complete review of the current No Fly list holdings is being conducted to update records. On June 1st TSA began receiving nominations through the TSC rather than in the form of individual cables, FAXs, and letters from agencies. This transition effort is a top priority for my intelligence team.

INTELLIGENCE OFFICE

88. How do you envision the role of the intelligence office which used to be part of FAA, then TSA, and now is a part of the Intelligence Analysis and Infrastructure Protection (IAIP) directorate at DHS? Is that office's primary responsibility to TSA or to the IAIP directorate?

Answer: The Transportation Security Intelligence Service (TSIS) is the intelligence organization for the Transportation Security Administration, and is one of several intelligence elements within DHS. TSIS fully coordinates its activities with the Information Analysis and Infrastructure Protection directorate (IAIP) within DHS, as do all DHS intelligence elements. TSIS is an all-source intelligence analysis program. Its

primary responsibility, as called for in ATSA, is to receive, assess, and distribute intelligence related to transportation that is focused on threats to transportation security. The TSIS mission is to provide timely, value-added intelligence analysis on US transportation security issues. Its objectives include assuring that:

- TSA field operations, including the Federal Security Director (FSD) and Transportation Security Area Representative (TSAR) programs, receive the threat intelligence they need to protect the infrastructure and operations for which they are responsible. TSIS also supports the Federal Air Marshal (FAM) program by Memorandum of Agreement;

- TSA leadership has domain awareness of the transportation security environment here and abroad;

- TSA security operations groups receive intelligence information that assists in security policy making and countermeasures planning; and

- TSA's private sector stakeholders have the threat intelligence that they need to make informed security decisions about their assets and operations and to work more effectively with TSA's representatives in the field.

89. Do you anticipate any needs in the intelligence area related to TSA's responsibilities that may demand a higher priority than they are now receiving?

Answer: I do not anticipate any at this time, as TSA's intelligence responsibilities already receive the highest priority in the agency. However, we continually evaluate our needs.

IV. Relations with Congress

90. Do you agree without reservation to respond to any reasonable summons to appear and testify before any duly constituted committee of the Congress if you are confirmed?

Answer: I do so agree.

91. Do you agree without reservation to reply to any reasonable request for information from any duly constituted committee of the Congress if you are confirmed?

Answer: I do so agree.

V. Assistance

92. Are these answers your own? Have you consulted with the DHS, TSA or any interested parties? If so, please indicate which entities.

Answer: These answers are my own. I have consulted with senior staff within TSA on preparing these answers, including Counsel. I have also had standard pre-confirmation discussions with staff at DHS, the Office of Government Ethics, and the White House Personnel Office.

AFFIDAVIT

I, _____, being duly sworn, hereby state that I have read and signed the foregoing Statement on Pre-hearing Questions and that the information provided therein is, to the best of my knowledge, current, accurate, and complete.

_____

Subscribed and sworn before me this _____day of _____, 2004.

_____
Notary Public