NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

Search

Seventh public hearing of the National Commission on Terrorist Attacks Upon the United States

Statement of James M. Loy to the National Commission on Terrorist Attacks Upon The United States
January 27, 2004

Good afternoon, Chairman Kean, Vice Chairman Hamilton, and distinguished Members of the Commission. I am pleased to appear before you to discuss the significant improvements in transportation security being made by the Department of Homeland Security (DHS) and the efforts of the Transportation Security Administration (TSA) in establishing a new aviation security regime.

You have asked me to focus in particular upon TSA's role in setting and enforcing transportation security policy while I served as Administrator. In the summer of 2002, when I assumed leadership at TSA, the agency's immediate mission was clear. We were charged

Current News

The Commission has released its final report. [more]

The Chair and Vice Chair have released a statement regarding the Commission's closing. [more]

The Commission closed August 21, 2004. [more]

Commission Members

Thomas H. Kean
Chair

Lee H. Hamilton
Vice Chair

with rebuilding and reinvigorating our civil aviation security system, providing world-class customer service, and restoring confidence in air travel. We were challenged with standing up a new organization and fulfilling the rigorous requirements of the Aviation and Transportation Security Act (ATSA). Secretary of Transportation Norman Y. Mineta was firm in his conviction that each and every ATSA deadline would be met.

The 30-year-old security system TSA inherited was focused chiefly on efficiency. TSA, with the help of its many partners, endeavored to create a new aviation security system that was dramatically different from the system in place on September 11, 2001. TSA's fundamental strategy was to establish a system of rings of security whereby each security ring contributes to our overall aviation security system but we do not rely exclusively on any one component (see attachment for a diagram depicting the aviation rings of security).

Today, TSA continuously gathers as much information as possible about the threats, vulnerabilities, trends, and conditions of the aviation system and its environment. This first ring in our system-of-systems, domain awareness, enables TSA to prioritize, direct resources, and take protective action. TSA and the Federal Aviation Administration (FAA) have helped fund many local airport projects to improve perimeter security, such as construction of perimeter access roads, installation of access control systems, electronic surveillance and intrusion detection systems, and security fencing. TSA has required background checks to be performed on more than a million air carrier and airport employees with unescorted access to airport secured and sterile areas. At checkpoints, highly trained, qualified personnel screen every passenger and bag using metal detectors and X-ray technology. Since February 2002, for example, TSA has intercepted more than 1600 firearms and more than 58,000 box cutters. We take pride in the

professionalism and diligence shown by TSA screeners every day in their efforts to ensure the security of the traveling public.

All checked baggage is screened using a combination of explosives detection systems (EDS), explosives trace detection machines (ETD), and where necessary, other congressionally approved methods of screening. TSA-certified canine teams perform multiple tasks throughout the entire airport environment, including screening checked baggage, searching unattended bags, searching vehicles approaching terminals during increased threat levels, screening cargo on a limited basis, and responding to bomb threats. The number of Federal Air Marshals (FAMs) has increased from just a handful on 9/11 to thousands today, and they are now deployed on high-risk domestic and international flights. With the recent transfer of the FAM Service from TSA to the Bureau of Immigration and Customs Enforcement (ICE), DHS will have the flexibility to deploy additional ICE agents as a surge force to temporarily increase the number of deployed FAMS on high-risk flights when threat conditions warrant. Commercial aircraft serving the U.S. are equipped with new, hardened cockpit doors. The Federal Flight Deck Officer program trains, equips, and deputizes pilots who volunteer to defend the flight decks of passenger aircraft as the last line of defense. By the end of Fiscal Year 2004, at the current pilot application rate, TSA expects to have trained the vast majority of pilots who have volunteered for the program and met the initial background requirements.

Each of these security enhancements is an additional obstacle that a terrorist would have to overcome in order to accomplish his objective. Each has been carefully developed with attention to security, customer service, and a minimum impact on the flow of commerce.

I would like to highlight the critical role of security intelligence in our overall security

strategy. TSA receives intelligence information from many sources, from the intelligence community and law enforcement, and from our own Information Analysis and Infrastructure Protection Directorate (IAIP), which has overall responsibility at DHS for receipt and analysis of information related to threats to the homeland. TSA's Office of Intelligence details the type of information TSA needs to intelligence collector agencies, and both raw and analyzed information are provided to TSA based on these statements of interest. TSA also has electronic connectivity to intelligence community databases and participates in daily intelligence teleconferences with other Federal agencies to discuss threat and incident reports. To ensure that all information pertinent to transportation security is identified and provided to TSA on a timely basis, TSA has assigned liaison officers to several Federal and law enforcement agencies. TSA has two assignees at the Terrorist Screening Center (TSC) adjudicating nominations for TSA watch lists and is supplying detail personnel to assist in TSC call center operations. The TSA Transportation Security Coordination Center (TSCC) was activated in 2003. The National Capital Region Command Center is co-located with the TSCC and provides a seamless integration in protecting the National Capital Region. In addition to intelligence information, TSA field personnel report information from local law enforcement and on security incidents at airports and aboard aircraft. TSA evaluates their intelligence value and shares them with the intelligence and law enforcement communities. TSA coordinates with IAIP to disseminate specific warning or advisory information to local law enforcement and the aviation industry.

All threat information received by TSA, including information not specifically mentioning transportation, is carefully reviewed for its potential impact on any U.S. transportation assets. Many factors are taken into account in assessing threat information, such as the history

of those making the threat, their capabilities and operations, their motivation, and their locations. TSA coordinates with all DHS Directorates to consider security measures already in place and the status of targeted transportation assets to determine the viability of the threat and the likelihood that a terrorist would be successful. The collector agency's assessment of the credibility and reliability of the information is considered as well. TSA also consults with other security and technical experts within DHS and in other agencies to achieve a comprehensive threat and vulnerability assessment.

If we conclude that warning to industry and field operators or operational adjustments are warranted, our response can take a variety of forms. Almost immediately, top government decision makers are alerted, as well as industry stakeholders. TSA operates a round-the-clock Transportation Security Coordination Center (TSCC) that serves as a single point of contact for security-related operations, incidents, or crises in all modes of transportation. TSA's 24-hour watch routinely alerts industry representatives to events or information of potential interest. If broader or more detailed warnings are necessary, threat information is distributed through a number of written products, such as Information Circulars, which provide information of concern to the transportation community, or Security Directives or Emergency Amendments, which provide specific guidance on security measures that must be implemented by regulated industry stakeholders. One of the most prominent ways TSA identifies potential threats to industry stakeholders is through dissemination of watch lists, which include individuals known or believed to be a threat to civil aviation. In addition, TSA produces several classified and unclassified daily products, all of which provide information on current topics of intelligence and security interest for TSA and DHS field and headquarters personnel.

Across the country, 158 Federal Security Directors (FSDs) lead and coordinate all TSA security activities at airports, including tactical planning, execution, and operating management. These individuals have had distinguished careers; their ranks include Flag Officers from Military Departments, career law enforcement officers from the FBI, Secret Service, Drug Enforcement Administration and other Federal agencies, and top industry executives.

An important responsibility for FSDs is the coordination of security measures based on changing threat levels. When the nationwide threat level was raised, TSA issued direction to FSDs, airport operators, and airlines to increase aviation security across the board. Additional security measures were implemented according to specific threat information. We have a large range of security measures that can be taken to counter specific threats, such as those tied to a location, an airport, or an air carrier, without affecting the entire transportation system. You saw this system in effect during the recent increase to threat level Orange, and the actions that TSA and DHS took with respect to high-risk international flights. TSA and DHS sister agency U.S. Customs and Border Protection maximized anti-terrorist efforts in the air environment by coordinating air security operations. Combined agency resources were utilized to screen passengers, cargo, aircraft and airport personnel with access to aircraft. Not only did DHS work closely with intelligence and law enforcement agencies to assess the threat, but we received invaluable cooperation and assistance from the State Department in addressing issues with our international partners. I would also be remiss if I did not acknowledge the close cooperation and assistance rendered by the Department of Transportation and the FAA in addressing this serious threat to homeland security.

The importance of private sector involvement in

the design and implementation of security countermeasures cannot be overstated. Security is a partnership, and we hold transportation stakeholders responsible for their contribution to security. Air carriers, airports, and transportation operators are complying with TSA security directives, although FSDs are working to improve consistency in some areas. TSA has adopted a progressive enforcement policy that emphasizes immediate corrective action and compliance before pursuing traditional enforcement through the imposition of civil penalties.

Cargo security on passenger aircraft is a concern for all of us engaged in transportation security. As Secretary Ridge has announced, TSA security directives now require random inspection of air cargo and require foreign all-cargo air carriers to comply with the same cargo security procedures that domestic air carriers must follow. These actions are building blocks in a comprehensive Air Cargo Strategic Plan that uses a threat-based, risk managed approach. The Plan is based on recommendations of working groups of TSA's Aviation Security Advisory Committee, as well as recommendations of the General Accounting Office (GAO) and the Department of Transportation's (DOT) Office of Inspector General.

TSA's actions have not been limited to aviation security. Last year, during the conflict with the regime of Saddam Hussein, TSA participated in Operation Liberty Shield, a comprehensive program to protect the public safety and critical infrastructure from attacks. TSA prepared security directives that would have been issued to owners and operators of all surface transportation modes in the event of actionable intelligence. TSA has also responded to bomb threats against bus tour operators and tips concerning trucks loaded with explosives.

Implementing a Risk Management System

TSA has developed and is implementing a suite of risk management tools to use in the development of transportation security strategies. Based on the risk-management approach recommended by the GAO and working with the IAIP, TSA is working to ascertain the threats, probabilities, and consequences of potential attacks on transportation systems. TSA's tool suite consists of a criticality tool, a facilitated vulnerability assessment tool, and a vulnerability self-assessment tool. In conjunction with IAIP, TSA is currently evaluating transportation infrastructure assets in all modes of transportation using the criticality model (incorporating IAIP tenets) to identify national critical infrastructure. Assets are being evaluated in concert with DOT modal administrations and industry stakeholders. The analysis of vulnerability assessments begins with the identification of high impact threat scenarios—those with a high likelihood of occurrence, high consequences, and low security countermeasure effectiveness. Using the results, we can collectively develop targeted, layered security measures tied to DHS risk levels with maximum flexibility to allow for normal transportation activity.

However, risk analysis and vulnerability assessments are just part of the broad spectrum of analytical activities that must be undertaken to develop a national homeland security strategy. We must design a security strategy for a significantly broader spectrum of responsibilities than we considered in the pre-9/11 world, ranging from enhanced awareness, through prevention, protection, response, consequence management, and recovery. To achieve this we need to develop more modern analytical tools. We need to do an even better job of gathering and analyzing information to improve our awareness, so that we can ultimately do a better job of designing prevention measures.

Looking to the Future

At the Coast Guard, I greatly admired core values that were so completely internalized—honor, respect, and devotion to duty. One of my first actions at TSA was to work with leadership to develop our own set of core values. They are:

- Integrity—We must be honest in dealing with the traveling public and inspecting their property;
- Teamwork—It takes great teamwork to perform effectively at the security checkpoints; and
- Innovation—What is being done today is not good enough for tomorrow. To be successful in its mission, TSA must internalize a culture of continuous improvement.

TSA was remarkably effective in grasping the principle of constant improvement. There has been no pause in the sense of immediacy felt at TSA, and there are several major improvement efforts underway that I would like to call to your attention.

We need to stay at least one step ahead at all times in the development of new security technology. Technology is an absolute necessity in detecting threats. TSA has a robust research and development program and works closely with the DHS Science and Technology Directorate to develop and deploy technology that will help make operations more effective, more efficient, less time consuming, and less costly. TSA has a state-of-the-art research laboratory, the Transportation Security Laboratory, located in Atlantic City, New Jersey. To help screeners better identify explosives and weapons that an individual may attempt to carry into the cabin of an aircraft, TSA is testing two explosives trace detection portals that analyze the air for explosives as passengers pass through them. TSA has also established a new

performance standard for walk through metal detectors (WTMD) and replaced every WTMD at all U.S. commercial airports with the latest technology. TSA is developing a document scanner that will detect traces of explosives on a boarding pass type document handled by a passenger. “Body scan” technologies, such as backscatter X-ray, millimeter wave energy analysis, and terahertz wave technology are also being evaluated, but deployment of any of these technologies will not proceed until sufficient safeguards are put in place to ensure the protection of passenger privacy.

TSA is continuing to work on identifying the next generation of explosives detection equipment for use in screening carry-on and checked baggage. TSA works with the vendors of the currently deployed technology to develop enhancements to existing EDS platforms to improve alarm rates, throughput, and reliability. Work is also underway with new vendors to develop technologies that will enable us to detect explosives in smaller amounts than are currently established in TSA’s certification standard and will occupy a smaller footprint at already overcrowded airports. TSA is looking at new applications of X-ray, electro-magnetic, and nuclear technologies to better probe sealed containers for materials that pose a threat.

TSA constantly assesses its own vulnerabilities and is currently moving forward on a plan to improve screener performance. TSA conducts an aggressive covert testing program that challenges screeners to detect threat objects at screening checkpoints and in checked baggage using simulated terrorist threat devices and current techniques. TSA conducts covert testing at over three times the annual rate of the old FAA “red teams,” and this testing uses more difficult, realistic testing situations. Concrete steps, including changes to training or standard operating procedures, are taken to address areas where performance can be improved.

Last July, TSA conducted a Screener Performance Improvement Study to determine the root causes for deficiencies in screener performance. After identifying the desired level of screener performance, TSA gathered data from multiple sources to determine the actual, current level of performance and the root causes for the gap between desired and actual performance. Based upon the Screener Performance Improvement Study, TSA identified an array of specific follow-up actions. These enhancements are now being implemented under TSA's Short-Term Screening Improvement Plan.

The screening improvement plan includes a major initiative to implement an enhanced version of the Threat Image Projection (TIP) system. TIP superimposes threat images on x-ray screens during actual operations and records whether or not screeners identify the threat object. This tool is excellent for evaluating the skills of each individual screener so that we can focus directly on areas needing skill improvement. By regularly exposing screeners to a variety of threat object images, TIP provides continuous on-the-job training and immediate feedback and remediation. TIP allows supervisors to closely monitor screener performance and improvement.

Although ATSA mandated the federalization of airport security screening, it held open the possibility that airports could return to contract screening, provided the high standards required of the Federal screening system could be met. TSA is currently operating a pilot program at five airports using private screeners that, by law, must meet TSA eligibility, training, and performance requirements and receive pay and other benefits not less than those of TSA screeners. Beginning on November 19, 2004, any airport operator may apply to have screening performed by a contract screening company under contract with TSA. One of TSA's key challenges in 2004 will be designing

appropriate criteria for the potential expansion of contract screening. To help TSA make these decisions, a contract has been awarded to conduct a thorough assessment of the pilot program.

Finally, TSA is well on its way toward implementation of another important tool in its system-of-systems of security, the second-generation Computer Assisted Passenger Prescreening System (CAPPS II). CAPPS II will greatly enhance TSA's ability to prevent terrorists from boarding commercial airlines while preserving the efficient flow of passengers. It will also help focus screening resources where they will be used most effectively. CAPPS II is intended to authenticate travelers' identities and perform a risk assessment to detect individuals who pose a terrorist-related threat or are subject to an outstanding warrant for violent criminal behavior before they board commercial airplanes. CAPPS II operates in two parts. First, it seeks to verify the identity of every passenger by matching limited information about the traveler, including name, date of birth, address, and phone number, with commercially available information. This check is done between databases outside a government firewall. CAPPS II will not bring any information found in the commercial databases into the government's system. Secondly, CAPPS II also performs a risk assessment, including a check against lists of terrorists and known or suspected threats, to detect individuals who pose a terrorist-related threat or are subject to an outstanding warrant for violent criminal behavior. Once the system has computed a traveler's risk score, it will send an encoded message to be printed on the boarding pass indicating whether the traveler is a green (no risk), yellow (unknown or elevated risk), or red (high risk). Eventually, this information should be transmitted directly to TSA screeners at security checkpoints. CAPPS II will be a threat-based system under the direct control of the Federal government and will

represent a major improvement over the current CAPPS system where information is decentralized and under the control of airlines.

In developing CAPPS II, DHS is very mindful of the rights, liberties, and freedoms that define our Nation and differentiate our society from those who seek to harm us.

CAPPS II is being designed and will be built with the explicit requirement that privacy protection not become a cost of increased aviation security. CAPPS II is undergoing a rigorous course of testing and will not be implemented until it has successfully passed this test phase.

In closing, I want to raise a word or two of caution. After the end of the Cold War, there was a period of complacency, a time when we assumed that our ability to address the Soviet threat had made us impervious to other threats. We must recognize the current potential for a similar period of complacency and guard well against it. This includes committing the resources necessary to establish and sustain our system-of-systems. At DHS, I can assure you we will press on, and we ask that our public and private sector partners stay the course with us.

Thank you again for this opportunity, and I will be happy to answer any questions you may have.

On December 4, 2003 Admiral James Loy was sworn in as the Deputy Secretary of the Department of Homeland Security. Admiral Loy formerly served as the Administrator of the Transportation Security Administration until he was nominated by President Bush in October.

On November 22, 2002, Congress confirmed Admiral James M. Loy as Under Secretary of Transportation for Security, within the Department of Transportation.

Admiral Loy retired from the Coast Guard as its Commandant on May 30, 2002. Transportation Secretary Norman Y. Mineta immediately appointed him to the newly created post of Deputy Under Secretary for Transportation Security and Chief Operating Officer of TSA.

As Commandant of the U.S. Coast Guard from May 1998 to May 2002, he focused his leadership on restoring readiness and shaping the future. Although both themes involved many initiatives, the most visible expression of restoring readiness was rebuilding the Coast Guard's workforce to authorized levels, improving retention and managing operational tempo. The primary element for shaping the future was his oversight and leadership in the Integrated Deepwater System acquisition project, which will modernize the ships, aircraft, and sensors that the Coast Guard uses to perform its many open ocean missions.

Prior to his service as Commandant, Admiral Loy served as the Coast Guard Chief of Staff from 1996 to 1998, during which time he redesigned the headquarters management structure and overhauled the Coast Guard planning and budgeting process to focus more sharply on performance and results. From 1994 to 1996, he was Commander of the Coast Guard's Atlantic Area, leading U.S. forces during the mass Haitian and Cuban migrations of 1994, and leading Coast Guard forces participating in Operation Restore Democracy. His other flag assignments included Chief, Office of Personnel and Training, and Commander, Eighth Coast Guard District.

A career seagoing officer, Admiral Loy has served tours aboard six Coast Guard cutters, including command of a patrol boat in combat during the Vietnam War and command of major cutters in both the Atlantic and Pacific Oceans.

Admiral Loy graduated from the U.S. Coast Guard Academy in 1964 and holds two master's

degrees, one from Wesleyan University and one from the University of Rhode Island. In 2003, he received the Honorary Degree in Science from the Webb Institute. He also attended the Industrial College of the Armed Forces and interned at the John F. Kennedy School of Government at Harvard University. His commendations are numerous, including the Department of Transportation Distinguished Service Medal; four Coast Guard Distinguished Service Medals; the Defense Superior Service Medal; the Bronze Star with Combat "V"; the Combat Action Ribbon; and other unit and campaign awards.

Admiral Loy was named SEATRADE Personality of 2000 in London, UK, has received the NAACP Meritorious Service Award for 2000, and was recognized by the Soldier's, Sailor's, Marine's and Airmen's Club with its Military Leadership Award for 2001. The American Society of Public Administration and the publication, Government Executive, recognized Admiral Loy with their Leadership Award for 2001.

The Reserve Officer Association inducted Admiral Loy into its Minute Man Hall of Fame. Most recently, he received the National Cargo Security Council National Leadership Award for 2002, and was honored with the Seaman's Church Institute Silver Bell Award. He also received the Navy League prestigious Admiral Arleigh Burke Leadership Award for 2002.

Admiral Loy is married to the former Kay McGirk. They have two grown children, Kelly and Michael. The Loys have two grandchildren.