Statement of Claudio Manno
Assistant Under Secretary for Intelligence
Transportation Security Administration
before the
Senate Select Committee on Intelligence
and
House Permanent Select Committee on Intelligence

October 1, 2002

Mr. Chairman and Members of the Select Committees, I am pleased to represent the Department of Transportation and participate in your joint inquiry into the performance of the intelligence community concerning the September 11, 2001, terrorist attacks against the United States. My statement addresses questions posed in your letter of invitation.

You asked about the policies and procedures in place at the Department to receive and act on intelligence information from the Intelligence Community and law enforcement organizations concerning terrorism. It is helpful to look at this issue first in terms of how intelligence relating to terrorism flows from producer agencies of the Intelligence Community to the Department of Transportation (DOT), including the Office of the Secretary, the Federal Aviation Administration (FAA) and the Transportation Security Administration (TSA). The second part of the process concerns how (and how much) information from the Intelligence Community is passed to state and local law enforcement agencies, as well as the private sector.

The mechanisms for passing information by the Intelligence Community (IC) to DOT are well established. DOT (including the Office of the Secretary, FAA and TSA) identifies and updates its intelligence needs in detailed "statements of intelligence interest" or "reading requirements," which the IC producer agencies keep on file to determine which products (both raw intelligence and finished products) DOT receives. To help ensure that the Intelligence Community agencies share pertinent intelligence fully with DOT, section 111(a) of the Aviation Security Improvement Act of 1990 (P.L. 101-604) required "the agencies of the intelligence community [to] . . . ensure that intelligence reports concerning international terrorism are made available . . . to . . . the Department of Transportation and the Federal Aviation Administration." The agencies responsible for producing most of the intelligence DOT receives on terrorism are the Central Intelligence Agency (CIA), the Department of State (DOS), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the Defense Intelligence Agency (DIA).

DOT, especially through TSA, is a full and active participant in the national counterterrorism and law enforcement communities by virtue of its relationships with these agencies. A full-time CIA liaison is posted to the Secretary's Office of Intelligence and Security, and that office has established a part-time liaison position at FBI. FAA has also provided a DOT liaison officer to the National Infrastructure Protection Center at FBI. TSA's Transportation Security Intelligence Service (TSIS) maintains full-time

liaison officers at FBI Headquarters, the CIA Counterterrorism Center, and Diplomatic Security's Office of Intelligence and Threat Analysis at DOS. TSIS plans to post liaison officers in the near future at NSA and DIA as well.

The Office of Intelligence and Security (S-60) has historically been responsible for providing intelligence support to the Secretary of Transportation and his staff, and to the DOT Operating Administrations that do not have organic intelligence capabilities such as FAA and Coast Guard have. Unlike TSA, S-60's current focus is on satisfying the intelligence needs of the Department of Transportation's highest level decision-makers. S-60 still coordinates the intelligence and security needs of the Secretary's Operating Administrations (FRA, FTA, MARAD, Office of Pipeline Safety, FMCSA, and FHWA), along with the IC (FBI, CIA, NSA, DIA), and other federal, state, and local agencies, and private industry.

With respect to transportation modes other than aviation, many of the responsibilities now being assumed by TSA had previously been discharged by S-60. At present, S-60 continues to share information with industry, depending on its sensitivity, either via the Transportation Security Information Report (TSIR) or over a secure telephone. The TSIR is an unclassified product meant for wide distribution to security officials within the transportation sector. The content of the TSIR is generally derived from classified intelligence. If the information cannot be declassified, it is transmitted by secure telephone to representatives of the affected industry who hold the proper security clearance. TSIRs prepared by S-60 are routinely coordinated with TSA and others in the law enforcement and intelligence community.

Until the passage of the Aviation and Transportation Security Act (ATSA), DOT distribution of threat information was severely limited because some of the information had to be disseminated without being protected from release into the public domain. Only the FAA had sufficient authority to share "sensitive security information" (SSI) with the private sector. The ATSA broadened the scope of the FAA's SSI authority and will now give DOT and TSA a much better tool to send sensitive threat related intelligence information to all affected transportation modes.

In addition to the previously mentioned liaison officers, S-60 and TSIS analysts routinely deal with their counterparts at the CIA, FBI, DOS, and the Department of Defense (DOD) at conferences, meetings, and working groups such as the Interagency Intelligence Committee on Terrorism and its subcommittees. Two TSIS analysts are assigned to the National JTTF at FBI Headquarters, and liaison initiatives are also underway to assign TSA criminal investigators to FBI Field Office Joint Terrorism Task Forces (JTTFs). TSA is currently identifying which JTTFs around the country would be best suited for TSA participation. A comprehensive TSA Statement of Investigative Interest is being developed, and consultations with the FBI will be undertaken to finalize a Memorandum of Understanding that reflects TSA's operational and information requirements.

The TSIS officers detailed to DOS, CIA, and the FBI meet the same high personal and professional standards as the regular employees of these agencies. Accordingly, they are fully integrated into these agencies and have the same access and restrictions as the agencies' own employees. This access includes the ability to read and review information that is disseminated externally to other agencies, as well as internal, operational, "in-house" e-mails and message traffic that is not shared with outside agencies. As a result, TSIS liaison officers may know more about a terrorist threat or incident than they are allowed to disclose, and TSIS understands that this is the tradeoff for those agencies' granting the liaison officers access to their information. TSIS fully concurs with such restrictions when they are based on the "need- to-know" principle and the requirement to protect intelligence and law enforcement sources and methods.

Where TSIS has had issues with this arrangement is in the definitions used by those agencies of what constitutes need-to-know for TSA. For example, threat information is routinely shared with TSIS, whereas domestically acquired non-threat information (such as terrorist group presence, intentions, and capabilities) needed to evaluate the threat information is provided less often, because it is considered investigative or law enforcement material rather than intelligence.

Unlike CIA, DOD, and DOS, the FBI has not historically considered itself an intelligence production agency due to the statutory restrictions on the dissemination of information it collects in its investigative role.

TSIS has experienced no significant intelligence-sharing problems with DOS or DOD. With respect to the CIA, those few times where TSIS has had problems resulted from unfamiliarity on the part of CIA personnel with FAA's (now TSA's) mission, roles, and responsibilities.

On a daily basis, S-60 and TSIS receive a steady stream of raw reporting and finished intelligence from DOS, CIA, and DOD. This flow includes items that are sent electronically, hard-copy products received via courier, and cables and finished intelligence TSIS can access and retrieve using INTELINK. In addition, e-mail communications with TSIS liaison officers and the staff of other agencies are sent and received using both classified and unclassified systems. From this inflow, TSIS Watch analysts identify, on average, between one and two hundred classified cables, reports, hard-copy products, faxes, and e-mails each day that merit closer review.

TSIS does not receive a similar flow of daily raw reports and finished intelligence from the FBI. It has received from the Bureau finished, summary intelligence on terrorist groups in the U.S. and an assessment of the threat these groups pose to domestic airports and air carriers. In addition, TSIS occasionally receives cable messages regarding potential threats to transportation or a response to a detailed question or request for assessment that TSIS may have requested via one of its liaison officers. Like other federal agencies, TSIS also receives the FBI's classified Terrorist Threat Warning Notices, intelligence bulletins, BOLO (Be On the Lookout) alerts, NLETS messages, the NIPC daily report, and the FBI's annual summary report of terrorism in the United States.

We expect, however, that the flow of raw background reporting from the FBI will increase in the future. The USA Patriot Act of 2001 authorized the sharing of criminal investigative information with other federal agencies in matters of foreign intelligence and counterintelligence, amending previous laws that had prohibited the FBI from sharing Grand Jury and FISA information. The Act also directs the Attorney General to establish procedures for the disclosure of such information. In October 2001, President Bush noted that the Act contained provisions to reduce the existing barriers to the sharing of information. He stated, "The ability of law enforcement and national security personnel to share this type of information is a critical tool for pursuing the war against terrorism on all fronts." As these changes in the law and in the guidelines become institutionalized in FBI policy, we anticipate an increased flow of intelligence.

The process of getting intelligence from DOT into the hands of those who need it for aviation security at the operational level (both state and local law enforcement and the affected private sector) has been accomplished at FAA (now TSA) primarily through the preparation and issuance of either Security Directives (SDs), Emergency Amendments (EAs), or Information Circulars (ICs). Occasionally, a strategic assessment of the terrorist threat is also disseminated to provide a general overview of the threat environment. Law enforcement officers responsible for security at airports have access to the threat information contained in SDs, EAs, and ICs, which is transmitted to them via the "Airport Law Enforcement Agencies Network" (ALEAN). This information is provided as unclassified, "sensitive security information," which in most cases consists of a declassified version of originally classified information. These declassified versions are prepared by the originating agencies with full knowledge of the intended purpose and recipients of the declassified language. Regulated aviation entities (air carriers and airports) receive the SDs, EAs, and ICs directly. In the case of SDs and EAs, the threat information is coupled with mandated security countermeasures that the air carriers or airport authorities must carry out. For example, watch-listed names are provided to airlines in one of two lists (one list is for individuals who should not be transported unless first cleared by law enforcement; another is for individuals who may be transported, but only after undergoing special security measures reserved for so-called "selectees"). The information is available to individual airline check-in agents, in either a manual or automated form, depending on the specific airline.

In addition to communicating threat information concerning aviation security via SDs, EAs, and ICs, TSA's 24-hour intelligence watch alerts industry representatives to events of potential interest that would not necessarily result in the issuance of SDs, EAs, or ICs. Furthermore, the intelligence watch sometimes relays pertinent information that cannot be declassified (regardless of whether it relates directly to the substance of an individual SD, EA, or IC) via secure telephone to properly cleared industry representatives. While TSA ensures that actionable intelligence is declassified and given broadest possible dissemination to those with a need-to-know, there are on occasion items of information that cannot be declassified, but that help industry decision-makers better understand the general threat climate or the context or rationale for mandated security measures. Thus, while there are no legal or policy obstacles to sharing information at the "sensitive

security information" level—indeed, the information is released in that form for the express purpose of sharing it—information that is classified must be protected in accordance with the laws governing the handling of national security information.

Mr. Chairman and Members of the Committee, we at the Department of Transportation recognize the significance of your efforts on behalf of the American people, and we appreciate the opportunity to participate in these proceedings. They will be significant in ensuring the future safety of our Nation. Thank you.