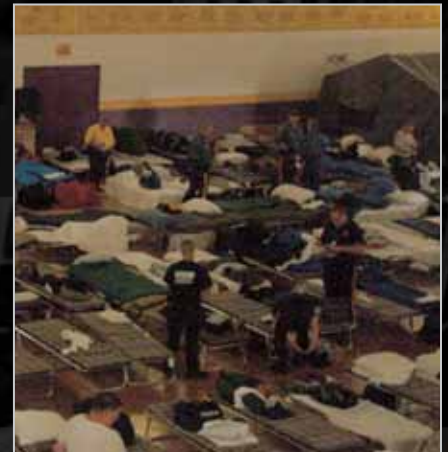


The Police Chief

THE PROFESSIONAL VOICE OF LAW ENFORCEMENT

FEBRUARY 2006



Inside:

Homeland Security

Preparing for a Pandemic

Quarantine: The Reality

Post-September 11 Policing

Tactical Information Sharing System

In the post-September 11 world, where the possibility of future criminal terrorist attacks remains high, the ability to identify criminal terrorist activity while still in the planning stages is vital. Consequently, the ability of law enforcement to detect pre-operational criminal terrorist planning has emerged as a cornerstone of homeland security. Recent examples of the importance of detecting criminal terrorist preoperational planning include the extensive preoperational surveillance conducted by the hijackers in the months preceding the attacks.¹

Recognizing that criminal terrorist activity involves some level of preoperational surveillance, federal air marshals are trained, and have extensive experience, in the art of surveillance detection—identifying criminal terrorist behavior and their surveillance activities while they are still in the planning stages. This proactive approach targets the criminal terrorist conducting surveillance during the planning stages in which they are most vulnerable to discovery. A federal air marshal must be prepared to make split-second decisions at 30,000 feet to thwart an attack, but the overriding objective is to keep the threat off the airplane.

The rail and bus bombings in London² underscore Homeland Security Secretary Michael Chertoff's philosophy that "our strength lies in what we can see and what we can access." If the London bombers' preoperational surveillance had been detected and accessible to law enforcement, the attacks might have been prevented.

The attacks of September 11, 2001, in the United States, the March 11, 2004, Madrid train bombings,³ the July 7, 2005, attacks in London, and the attacks in Indonesia⁴ and elsewhere create a mandate for law enforcement to enhance methods of detection, information sharing, and analysis to prevent future acts of violence.

To fulfill this mandate, the Transportation Security Administration's Federal Air Marshal Service (FAMS) has developed a comprehensive system that builds upon advancements in information technology and the talents of law enforcement officers trained to identify suspicious activities, potential threats, still in the planning stages, otherwise known as the art of surveillance detection.

Tactical Information Sharing System

The Federal Air Marshal Service Tactical Information Sharing System enables federal air marshals and other law enforcement officers to create and instantly send reports



*Thomas D. Quimm, Director,
Federal Air Marshal Service,
U.S. Transportation
Security Administration*

of suspicious activity to the Federal Air Marshal Service Investigations Division for analysis and investigation. The resulting surveillance detection reports (SDRs) are shared in real time with other federal, state, and local law enforcement and intelligence organizations. The key components of this Tactical Information Sharing System are the following:

- **Surveillance Detector:** A federal air marshal or other law enforcement officer who detects and reports the presence of suspicious activity possibly connected to criminal terrorist surveillance
- **Personal Digital Assistant (PDA):** The Federal Air Marshal Service's customized handheld electronic wireless device, with integrated SDR reporting software, issued to all federal air marshals for the purpose of submitting surveillance detection reports
- **Surveillance Detection Report:** An electronic form that surveillance detectors can use to record information of a suspicious nature and then transmit, using their PDAs, that information to the FAMS Investigations Division's Tactical Information Branch
- **Tactical Information Sharing System (TISS) Database:** The Internet-accessible database that stores information from surveillance detection reports, incident and arrest reports, and other sources for immediate retrieval and analysis
- **Tactical Information Sharing System Analytic Tool:** A data mining software application that enables analysts to uncover in the TISS database patterns, associations, and other indicators of possible criminal terrorist surveillance that requires further investigation

Surveillance Detection and Tactical Information Sharing System Training

The concept of surveillance detection and information sharing is woven into the fabric of the Federal Air Marshal Service's mission to detect, deter, and defeat hostile acts. Surveillance detection is a state of mind that begins when the federal air marshal leaves for work and does not end until he or she returns home.

Federal air marshals receive instruction in surveillance detection and Tactical Information Sharing System concepts throughout the 15-week federal air marshal training program and during periodic training conducted at each of the 21 field offices. Surveillance detection training includes instruction in terrorist methodologies, maintaining domain awareness, recognizing criminal terrorist surveillance, criminal terrorist behavior recognition, and fraudulent document identification.

Surveillance Detection Reporting and Analysis

Federal air marshals are constantly looking for suspicious behavior that may be early indicators of criminal terrorist surveillance activity. A single instance of suspicious behavior viewed in isolation may not be meaningful, but many instances of suspicious behavior viewed collectively can create a comprehensive picture. Possibilities become probabilities, when associations emerge across time, distance, and venue. Early indicators may be elements of significant criminal terrorist surveillance activity and planning.

Federal air marshals who observe suspicious activity use a customized personal digital assistant loaded with specialized software to capture and send surveillance detection reports to the Investigations Division. Surveillance detection reports may also be submitted through the Internet via a secure Tactical Information Sharing System Web site. This real-time collection and timely analysis of a federal air marshal's observations begins the process of connecting dots that may later form a picture of a criminal terrorist plot. Every federal air marshal and many other law enforcement and intelligence organizations have direct access to the Tactical Information Sharing System.

Once a surveillance detection report is recorded in the database, specialized data-mining software helps investigators and tactical information analysts identify associations, trends, and patterns requiring further investigation. The ability to link and analyze seemingly unrelated activities to develop information which reveals criminal terrorist planning is at the heart of the Federal Air Marshal Service Tactical Information Sharing System.

Tactical Information Sharing

Information contained in the Tactical Information Sharing System database is unclassified and defined as tactical information; this enables real-time information sharing. The Federal Air Marshal Service strategy involves openly sharing tactical information among local, state, and federal law enforcement agencies. Currently, 22 law enforcement and intelligence organizations have direct access to the Federal Air Marshal Service Tactical Information Sharing System.

Applying the Tactical Information Sharing System

The Federal Air Marshal Service Tactical Information Sharing System became fully operational in 2002. The following two real-world events serve to illustrate the capability that tactical information sharing offers law enforcement.

Suspicious Behavior: A federal air marshal submitted a surveillance detection report on two subjects who were together and behaving suspiciously by asking repeated questions about aviation operations at an airline ticket counter. Unknown to the federal air marshal at the time, both persons were independently known to federal law enforcement as persons of interest. Federal officers, through their access to the Tactical Information Sharing System, were able to establish a relationship between the subjects. Sharing information among agencies, and thus linking the subjects, provided vital information used during the ongoing investigation.

Attempted Security Breach: On two separate occasions, surveillance detection reports were submitted to the Tactical Information Sharing System database involving the same subject who attempted to pass through an airport security screening checkpoint with a handgun. Since the two attempts occurred at separate airports on separate dates, conventional reporting methods failed to link the incidents; fortunately, the Federal Air Marshal Service, using the Tactical Information Sharing System database, was able to establish a correlation between the incidents.

The Way Ahead

The capabilities of the Federal Air Marshal Service Tactical Information Sharing System continue to expand. One initiative in development makes use of the camera currently integrated into the Federal Air Marshal Service PDA. This approach, known as Tactical Information Sharing System Image Analysis, involves the submission of images in conjunction with surveillance detection reports for

the purpose of advanced comparison and analysis. These images may represent persons, vehicles, or other items of interest. Tactical Information Sharing System Image Analysis will be capable of manipulating partial images to create a full-face or profile image. The Tactical Information Sharing System Image Analysis capabilities are nearing completion and will be operational in 2006.

The TSA Federal Air Marshal Service is working to advance leading edge information sharing technology across local, state, and federal agencies. The Federal Air Marshal Service is committed to sharing critical information with our partners in the law enforcement and intelligence communities. By working together to design and implement a sophisticated Tactical Information Sharing System we can make the nation safer from criminal terrorist attacks on the homeland. ❖

Editor's Note: FAMS Director Thomas D. Quinn has announced his retirement effective February 3, 2006.

¹The 9-11 Commission Report: *Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition* (Washington, D.C.: U.S. Government Printing Office, (July 22, 2004); available at no cost at www.gpoaccess.gov/911/index.html.

²MIPT Terrorism Knowledge Base, "Incident Profile," July 7, 2005, www.tkb.org/Incident.jsp?incID=24394, December 23, 2005. The July 7, 2005, London bombings were a series of coordinated suicide bombings during the morning work rush hour on three London underground trains and one bus. The bombings killed 52 civilians and injured over 700 people.

³MIPT Terrorism Knowledge Base, "Incident Profile," March 11, 2004, www.tkb.org/Incident.jsp?incID=18518, December 23, 2005. The March 11, 2004, bombings killed 191 people and injured more than 600 when 10 bombs detonated in four different locations on Madrid's railway system.

⁴MIPT Terrorism Knowledge Base, "Incident Profile," August 5, 2003, www.tkb.org/Incident.jsp?incID=18621, December 23, 2005. A suicide car bomb detonated in front of a Marriott hotel in Jakarta, killing 13 people and injuring approximately 149 others. The adjoining office block and several cars caught on fire from the explosion. The attack came two days before a verdict in the trial of the Bali nightclub bombers. On October 12, 2002, three explosions rocked the resort island of Bali in Indonesia. More than 421 people were reported missing and it was confirmed that 202 people died in these blasts. See John Lawler, "The Bali Bombing: Australian Law Enforcement Assistance to Indonesia," *The Police Chief* 71 (November 2004): 14-21.