Studies in Intelligence Vol. 50 No. 3 (2006)

Intelligence and Airport Security

Intelligence in Homeland Security

Robert R. Raffel

A consistent thread in post-9/11 discussion of Intelligence Community reform has been the importance of finding ways in which the community can more effectively share what it knows with other public and private entities with security concerns and to learn from those entities. The following is a contribution in that vein from an expert in airport security. The journal welcomes others in the security field to continue this discussion in Studies. *—Editor*

"Could airport security officials properly use intelligence if they could receive it."

The role of intelligence in an airport environment has long been a subject of debate and uncertainty. How much intelligence is out there? Of what quality or usefulness is available information relative to airport security? Could airport security officials properly use intelligence if they could receive it?

Appropriate collection, analysis and dissemination of *information* useful to an airport is problematic enough; the availability and usefulness of *intelligence* is even more so.[1] Further, even given the availability of information, what *processes* have been, or need to be established to leverage the product into something useful? Despite these issues, which are daunting, there are avenues open to the airport security practitioner to

receive useful information and to maximize intelligence collection, reception and dissemination.

The Issues

Civil aviation has often been an area of terrorist interest and activity. Long before the events of 11 September 2001, terrorists targeted airports and aircraft. The Rome and Vienna massacres of 1985 were launched against airports themselves. The hijacking of TWA 847 that same year, together with a variety of attacks occurring before and after those events served to identify aviation with terrorism in the public mind. For the terrorist, civil aviation assets remain high-value targets. The vulnerability of general aviation, an area subject to little regulation or security oversight, adds other issues to the calculus of security.[2]

Orlando International Airport is the busiest airport in Florida and, having served more than 34 million passengers in 2005, the nation's 15th largest international gateway. (Photo courtesy of author)

Despite the historical connections between terrorism and civil aviation,

public discussion of how best to address issues of information and intelligence in this sphere has been drawn-out, confusing and inconclusive. Each aviation incident brings forth an outcry for better information and intelligence sharing; why, the critics ask, didn't we know more beforehand? Or, conversely, if you knew, why weren't we told?[3]

These issues are also discussed in the airport environment. Airport operators have long felt that timely information and intelligence sharing could help them in their handling of security operations. Proactive security managers realize the importance of preparedness: information outlining threats to airports can help reduce risk. However, most managers are constrained by their inability to access accurate, systematically collected and processed information and by staffing limitations. Little, if any information or intelligence is airport-specific and information that is broader in scope is seldom useful. Finally, an individual airport security coordinator (ASC), depending on his or her own interests and unique capabilities, may have access to varying sources of information.[4] However, the data are often captured on an ad hoc basis rather than in a coordinated, process-driven approach to information sharing and analysis.

Another discrepancy exists in the distinction between openly acquired information and classified intelligence involving the clandestine collection of data or the accumulation of potentially sensitive information. Given the technological explosion of the past decade, information of all types has become ever more readily accessible. In fact, the very availability of information creates a dilemma for the airport security analyst: it is often difficult to separate the useful from the merely repetitive. Intelligence, on the other hand, becomes restricted from public dissemination, is closely held and controlled, and subject to rigorous requirements governing need-to-know. Although efforts have been made at higher governmental levels to share classified information with airports, a lack of standardization and consistency—indeed, the absence of an organized program—have hampered communications.[5]

The issues then, are several:

- What types of information are helpful to the airport security operator?
- Is it feasible, or even appropriate, for the airport to receive *intelligence*?
- What organizations presently exist to facilitate this function?
- Finally, is there a system-wide approach or model that might be used to

facilitate the best use of these products?

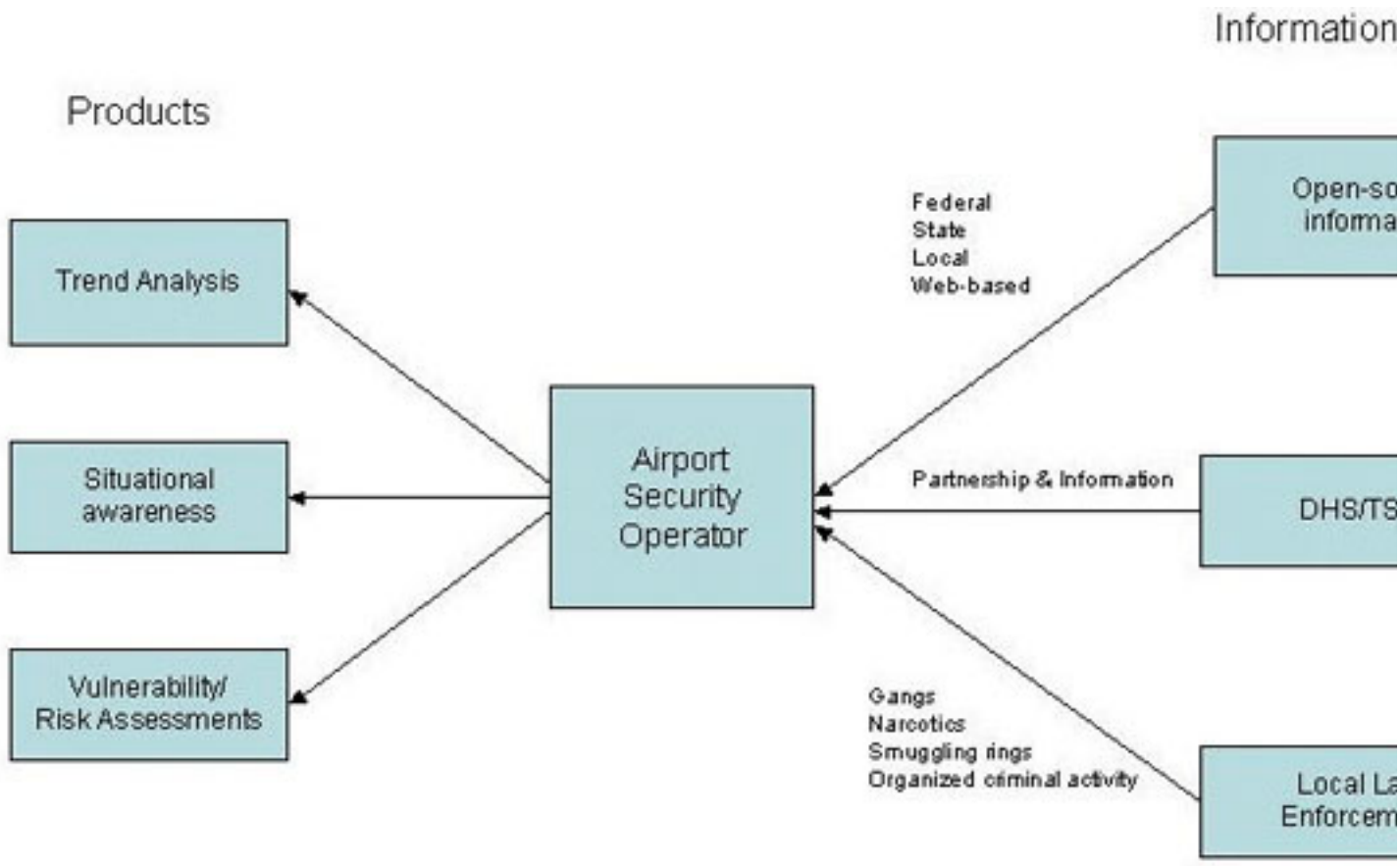
Open-source information

One of the products of our national effort to counter terrorism since 9/11 has been the application of various types of open-source information to airport security. Pre-9/11 information-sharing groups supporting airports, such as the Airport Law Enforcement Agencies Network (ALEAN), have organized to assist in this task.[6] In its Web page, ALEAN states one of its goals is to "facilitate the rapid exchange of information concerning airport-related crimes." Since 9/11, ALEAN has served as a conduit for information and open-source material directed primarily at the airport law enforcement manager and practitioner. Other national airport and air carrier organizations predating 9/11, such as the American Association of Airport Executives (AAAE), the Airports Council International–North America (ACI-NA), and the Air Transport Association (ATA), among others, have also served to facilitate the full and rapid flow of information to the airport and air carrier communities. Although these entities do not convey intelligence they nonetheless provide means by which useful facts may flow quickly to predesignated groups.

Since 11 September, other groups have formed, some with the primary purpose of forwarding information of use in counter-terrorist activities. One example is the Florida THREATCOM network, which functions at a state level. It is part of the state of Florida's Regional Domestic Security Task Force. It provides information and links for security and law enforcement practitioners. The Florida Department of Law Enforcement (FDLE) also mounts an informative page on domestic security, with a tip line to their Office of Statewide Intelligence.

Cognizant of terrorists' ability to leverage electronic information systems, Florida has also set up "Secure Florida", which seeks, as its Web page states, "To protect...Florida by safeguarding our information systems, reducing our vulnerability to cyber attacks, and increasing our responsiveness to any threat."[7] Groups such as these exist in many other states and throughout the Web, sponsored by everyone from federal and state organizations to think tanks to individuals. Finally, the Florida Division of Emergency Management publishes a daily status briefing,

which covers a wide range of topics of interest to the emergency management and law enforcement communities. Many other states have similar organizations that make such information available on a regular basis. The challenge in this area is to identify and prioritize sources that are helpful to the airport security manager.



The Airport Information-Sharing Environment

Local Intelligence

Given the lack of specificity involved with most national-level intelligence, the best information is often local. Most airports, especially those located near large population centers, have access to local law enforcement intelligence groups. Most law enforcement agencies now keep close track

of gang-related activity, for example. They also contain intelligence units that have the potential to provide useful information on airport-related activities of these groups and individuals, who also can do great harm. Given criminal activity at airports (e.g., narcotics and arms smuggling, organized and gang-related theft rings, etc.), area-specific information may actually prove better able to identify threats and thus be more useful than information at higher levels.

Another point in favor of paying close attention to local intelligence is that it tends to be more attainable. As mentioned above, most law enforcement agencies have criminal intelligence capabilities, which can be accessed and leveraged by the airport security manager. This information is especially helpful in airport vulnerability analyses, where thorough knowledge of threats helps produce a better understanding of risk.[8]

Some airport managers, recognizing the importance of this type of information, have established groups composed of local and federal law enforcement agencies that meet at regular intervals. At these meetings, principals discuss and exchange local threat information, status of current operations and other matters of mutual interest. Along with information exchanges, groups such as these benefit from the expanded network created and avail themselves of the opportunity to be woven into the tapestry of airport-related law enforcement. This is especially vital today, when an increasing number of law enforcement agencies are involved in aspects of airport security.[9]

Finally, airports themselves can leverage information collection opportunities. Most airport employees require ID media to accomplish their tasks, and airport security staffs receive information relating to each badged individual. This information, although subject to strict rules regarding dissemination, may be and has been used for counterterrorist and criminal investigations. Airport employees themselves, if given guidance and the right incentives, can be used as sources of information about suspicious activities and persons. Orlando International Airport, for example, has established close relationships with local police intelligence units. Gang activity is present both in the community and the airport, in itself a small city that tends to mirror the surrounding area. The airport-police partnership has resulted in the identification and arrests of suspicious individuals on several occasions.

DHS/TSA Information-Sharing Opportunities

Although the process is still evolving, TSA is working on methodologies to collect, analyze and appropriately disseminate intelligence to airports. The Federal Security Director (FSD) is the designated point of contact for the Airport Security Coordinator (ASC). This relationship is partly regulatory but is also a vehicle for sharing aviation-security-related information. [10] FSD's and ASC's who work to develop and cement close working relationships have a unique opportunity to engage in information and intelligence-sharing. In such an arrangement, the FSD gains the airports' insights into local threat groups and airport history with regard to terrorist and criminal activity. The airport, for its part, gains the FSD's access to wider sources of information.[11] Possibilities also exist in the area of vulnerability analysis. The FSD has the bigger picture and should be aware of national and international threat activity; the airport recognizes its inherent vulnerabilities. This situation is ideal for partnership and development of risk identification and mitigation strategies.

A good example of TSA airport coordination involved dissemination of information by TSA to airports concerning the threat of portable anti-aircraft missiles. Following a terrorist attempt to down a civilian aircraft over Mombasa, Kenya, in 2002, US officials began a concerted effort to educate local law enforcement and security officials about these weapons. TSA officials contacted airports and passed on information and graphics outlining the threat. Airports and their law enforcement entities then teamed with TSA, FBI, and other agencies to take remedial actions. Although the efficacy of this effort may be a matter of debate, it is an example of the possibilities of collaborative approaches to information-sharing.

Trend Analyses

One of the most valuable deliverables in a well-organized information-sharing environment involves trend analysis. Airports, as has been pointed out, are usually acutely aware of local events and, to a somewhat lesser extent, demographics. Governmental organizations, at local and federal levels, have a wider scope of information collection capabilities. The

opportunities for airport-local-federal partnerships abound. Using some of the collection sources mentioned above or by creating and leveraging new ones the security manager can attain unique capabilities. Information about seemingly unrelated activities can be collected, analyzed and culled for possible trends. Although some of this is already underway, greater emphasis can and should be placed on it.

The communications infrastructure to carry out the activity needed for effective trend analysis exists in various degrees of maturity. The civil aviation community, multifaceted and even chaotic to the untrained eye, is actually an interconnected network of entities that has spent years perfecting communications.

Some work of that type is being accomplished by different agencies, most at the federal level. A notable example is a new partnership program between elements of the Department of Homeland Security and local law enforcement. The program involves training local police to make and report spot observations. These reports are entered in a database available to other local and federal law enforcement groups around the nation. The database can be used to search for and produce information on similar events. As this program expands, the potential for trend analysis will grow exponentially.

This type of innovative approach to data collection and federal/local partnership is indicative of the wider federal vision involving airport security assets in addition to law enforcement.[12] These initiatives appreciably widen the intelligence collection effort and greatly enhance information gathering capabilities.

Conclusion

Information and intelligence are useful to the airport security practitioner. Much information is available through open sources, but challenges involve prioritization and analytical capability. Local intelligence, given the relative ease of collection and immediate applicability to the individual airport, has value to the airport security manager. Issues involving appropriate collection, analysis and utilization of information can be addressed through innovation and partnerships with local and federal actors. Even intelligence may be shared, given the proper foundation and

development of a suitable process. Finally, more work needs to be done in the area of trend analysis. The full realization of the potential in airport security assets is contingent upon leveraging existing infrastructures and designing a useful process for exploiting them.

Footnotes:

[1]*Information* used here in contrast to *intelligence*, as in the collection of "secret information" (*Webster's, Fourth Ed.).* For purposes of this article, the words *information* and *intelligence* shall be considered separately.

[2]General aviation aircraft and airports continue to grow in size and complexity. The growing popularity of fractional aircraft sales and rentals further adds to the complexity.

[3]This kind of information became an issue of debate after the bombing of PAA 103 on 21 December 1988. Investigators discovered that on 5 December 1988 a threat had been sent to the US Embassy in Helsinki, Finland. The threat stated that "some time within the next two weeks" a bomb would be placed upon a Pan Am flight flying from Frankfurt into the United States. This information was distributed selectively by the Federal Aviation Administration and the State Department, giving rise to the charge of "a double standard—the intentional choice to warn some people but not others." *Report of the President's Commission on Aviation Security and Terrorism, May 15, 1990.*

[4]Airport operators are required to designate an "airport security coordinator" (ASC) to (among other tasks) "...serve as the airport operator's primary ...contact for security-related activities and communications with TSA [Transportation Security Administration]". 49 CFR 1542, Sec. 1542.3.

[5]Following the PAA 103 bombing, the position of Federal Security Manager (FSM) was established, in line with the recommendations of the *President's Commission on Aviation Security and Terrorism*. One of the duties of the FSM was to "...serve as the conduit for all aviation-related intelligence." *President's Commission on Aviation Security and Terrorism, 60.* This function included the sharing of certain levels of classified information with designated civilian airport security managers, who were granted a security clearance by the FAA's Office of Civil Aviation Security. This program fell into disuse after the events of 9/11 and the subsequent transfer of aviation security responsibilities from FAA to TSA.

[6]Since its beginnings in 1990, ALEAN has grown to include over 85 domestic airports and several foreign airports. Information and training in airport-specific areas of interest to airport law enforcement officers has long been an ALEAN strength.

[7]Mission Statement, *Secure Florida* Web page.

[8]The model referred to here is the threat + vulnerability = risk equation. Airport security managers should know their airports' vulnerabilities; consequently, the more he or she understands about the threat, the more accurate the assessment of risk becomes.

[9]In the pre-9/11 airport security environment, FAA Federal Security Managers (see below) often developed such groups. Commonly called Threat Assessment Groups, or "TAG Teams", they played an important role in bringing law enforcement, information and airports together. Normally composed of federal, local and state law enforcement organizations having interests in and operations involving airports, they became a valuable tool for the Security Managers. Never formalized, this approach in most instances, did not survive the tidal wave of change that followed the US governmental response to the 9/11 attacks.

[10]The FSD position was created under the Aviation and Transportation Security Act (ATSA) Public Law 107-71. *See 49 USC, Section 44933.* Under the ATSA, each commercial service airport is assigned an FSD. The "legacy" position was the FAA's Federal Security Manager (FSM), itself formed by Public Law following the PAA 103 disaster. However, under the FAA, FSM's were never allowed the wide range of powers and authority that FSD's currently enjoy. The position of Airport Security Coordinator (ASC) predated that of the FSD, but was also recodified under the ATSA (*See Section 1542.3).* Under the ATSA, the ASC "Serves as the airport operator's primary and immediate contact for security-related activities and communications with TSA."

[11]Before 9/11, the FSM was authorized to share certain levels and types of classified information with the ASC, who was permitted to apply for the appropriate clearance through FAA. Although this arrangement fell into disuse after the events of 9/11 and subsequent reorganizations, there are indications that TSA is seeking to reestablish the process.

[12]Law enforcement and security are not synonymous terms, although DHS has often confused the two. For more detail on this subject, refer to

my article “Security and Law Enforcement: An Airport Model” in *Aviation Security International*, February 2005.

Robert T. Raffel is Senior Director of Public Safety for the Greater Orlando Aviation Authority and a member of the US Army Reserve. He has published articles in law enforcement and other journals on airport security issues.
