

# Access Control, Perimeter Security

TO BE ACTIVE TOPICS IN 2011

By Jeanne Olivier, A.A.E.

**A**ccess control and perimeter security at U.S. airports will receive renewed legislative scrutiny in 2011 as the House Committee on Homeland Security sets its agenda for the 112<sup>th</sup> Congress, according to Thomas McDaniels, committee senior professional staff member.

Complementary efforts are underway by TSA in its survey and compilation of *Best Practices and Innovative Measures* in airport security, as well as in the revision of the agency's 2006 document *Recommended Security Guidelines for Airport Planning Design and Construction*. To supplement the planning and design guidelines, TSA has commissioned a revision to the 2008 RTCA document, *Integrated Security System Standards for Airport Access Control*.

In addition, the independent AAAE Biometric

Airport Security Identification Consortium (BASIC) is developing a proposed Concept of Operations for the elective implementation of biometric credentialing and access control. Each of these efforts is supported by the voluntary work of airport managers, consultants and equipment manufacturers.

The House committee will report on the capability of access control and perimeter security measures at U.S. airports to meet anticipated security threats. Policies and operational procedures, as well as physical design and security equipment, are topics of review. The cost of and funding for airports to meet regulatory mandates and upgrade and maintain systems that keep pace with new threats will be factors in these discussions. The latest standards for such systems will be fundamental to any gap analysis on U.S. airport protection.

“As the security threat to airports continues to evolve, so does all of the planning, policies, procedures and technology intended to address it, and our standards and guidelines must reflect this evolution,” said Art Kosatka, coordinator of the Airport Security Design Guidelines Working Group of TSA’s Aviation Security Advisory Committee (ASAC). The guidelines are intended to help commercial airport operators ensure that security considerations and requirements are part of the planning and design of airport infrastructure, facilities and operations.

The revisions to the security guidelines for planning and design address all aspects of airport security from access control for secure areas to bomb blast considerations in public terminals, baggage screening, and so forth. The document provides background information on each topic to help designers and planners better understand the challenges that must be addressed at airports.

With respect to the technology and infrastructure aspects of airport access control, Kosatka noted, “There are no more green fields in the U.S. airports, so we are always retrofitting or expanding existing facilities. The usual expected life cycle of an access control system is six to seven years, but the technology and threats are evolving faster than that. So it is important that we design and use systems that are flexible, adaptable and

interoperable, to mitigate the cost of upgrading to meet new threat scenarios.”

Ann Barry, chair of the BASIC technical subcommittee and a contributor to the Security Design Guidelines Working Group, said, “We are often confronted with the challenge of not only compatibility and interoperability with legacy systems, but also of ensuring that interfacing to legacy systems does not compromise the full functionality of newly designed systems.”

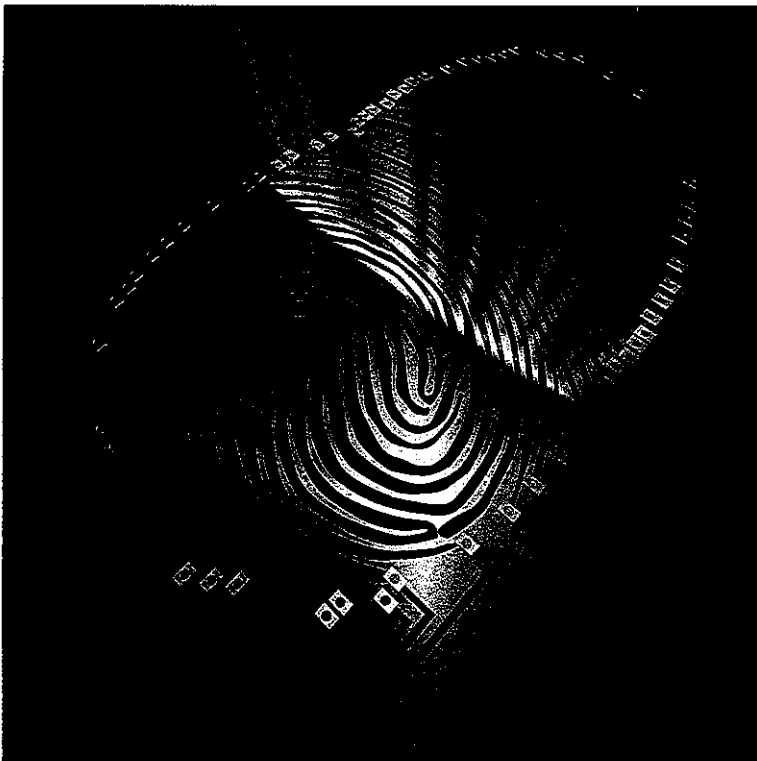
Cost and operational considerations often necessitate a phased transition to new security system elements, and the interoperability and flexibility of systems is important to the success of this move.

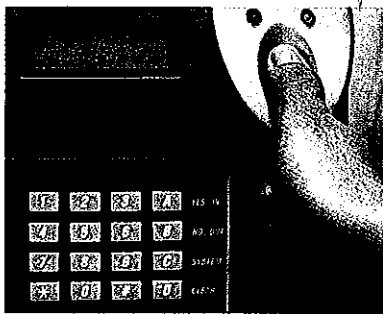
San Francisco International is in the process of upgrading its access control system. “The whole effort was propelled by our need to renovate and reopen an older terminal that had been vacant for a long time,” explained Kim Dickie, C.M., the airport’s director of security. “We had an older access control system that we were having trouble maintaining, and this presented the opportunity for us to improve our systems as we invested in the renovation of the terminal.”

The airport’s new system will incorporate biometric identification and prepare for future use of biometrics in access control. In developing contract specifications for its new system, San Francisco International drew upon the RTCA guidance on access control standards, and upon the BASIC committee’s exchange of lessons learned by colleagues from airports across the U.S. and Canada.

The revised RTCA document on access control standards will be referenced extensively in TSA’s security design guidelines document. The RTCA work provides minimum performance standards for the design of airport access control systems and other related electronic security systems and is referred to in determining requirements for AIP funding for such airport projects. Last issued in 2008, the document’s revisions will reflect the most current information on technology, regulations and standards, and will focus primarily on changes to federal and non-federal credentialing standards and common practices at airports.

The Concept of Operations developed by the BASIC committee to address legislative intent in biometric identification credentials for airport workers and biometric access control for secure areas will be included in the new RTCA guidance. The BASIC Concept of Operations is the airport





industry's collaboration for a practical approach to the transition to these higher levels of identity assurance. The RTCA standards updates are expected to be completed by June 2011. The committee will be co-chaired by TSA's Christopher Runde, the agency's director of aviation credentialing, and Christer

Wilkinson, senior project manager for AECOM/DMJM Aviation and a well-known technology consultant who chaired the last RTCA committee on this initiative. Meetings of the committee will be announced in the *Federal Register* and are open to the public.

Several years after their initial investment in access control technology, airports are seeking cost-effective ways to leverage their investments with component upgrades and further enhance the effectiveness of their security systems. The integration of many security components and related systems, such as door alarms, cameras, fire alarms and so forth, can provide security personnel with a highly desirable comprehensive situational awareness of their facilities, usually focused in a command and control center.

However, the closed nature of proprietary technology can impede the integration of new systems with legacy systems. In such cases, airports may choose to replace legacy systems with ones that have an open architecture and thus easily allow further expansion. Some airports are finding another option in the use of software products that sit between diverse systems and manage the communication among them.


Such direction in technology improvements will require financial investment and implementation strategies that may extend over a number of years. Airports will look to their colleagues, as well as to the consultant community, for advice based on their experiences in similar undertakings and for short-term initiatives that can offer improvements to their security program.

To understand which security strategies are operationally and financially practical, airports and Congress soon will be able to draw upon TSA's November 2009 survey of *Security Best Practices and Innovative Measures* of U.S. commercial airports. The survey report will highlight low-cost solutions to security requirements, as well as local initiatives that require more investment and contribute to higher levels of security control where the situation requires.

Douglas Hofsass, TSA deputy assistant administrator for transportation sector network management, is enthusiastic about the results of the survey. He commented, "The Best Practices and Innovative Measures initiative being led by TSA and strongly supported by airport operators is a true example of how strategic partnerships and collaboration can drive improvements in aviation security while creating efficiencies for airport operators.

"With more than 100 airports responding to the field survey, more than 700 best practices and innovative measures were submitted to TSA. Upon review, validation, and cataloging of these practices into a compendium/manual, airport operators will have a resource that can be referenced during capital planning, alternative measure reviews and internal efficiency studies. It is these types of 'real

results' that highlight how far the TSA relationship has evolved over the years with airports.

"Finding ways to improve security while reducing impact on airport operators is critical in a world of limited resources and a dynamic threat landscape," he added. 

Jeanne Olivier, A.A.E., is assistant director-aviation security and technology for the Port Authority of New York & New Jersey, and vice chair of AAAE's Transportation Security Services Committee. She may be reached at [jolivier@panynj.gov](mailto:jolivier@panynj.gov).

**aviation enthusiasts**  
for as long as we can remember...

- ▲ Engineering
- ▲ Construction Administration
- ▲ Planning
- ▲ Environmental Assessments

**DELTA AIRPORT CONSULTANTS INC.**  
[www.deltaairport.com](http://www.deltaairport.com)