tem. The key is to design and implement an intelligent storage scheme and use off-the-shelf storage rather than proprietary digital video recorders (DVRs) or network video recorders (NVRs).

Next Steps

For its part, the San Diego International Airport is in the conceptual phase of planning and architecting its next-generation security system and network. It is seeking best-of-class products at the edge and in the core, made interoperable by an IP network and a common application-programming interface (API) such as Extensible Markup Language (XML). With the video analytics beta tests concluded, the airport now needs to determine the size required for its servers and what type of backbone network would be most appropriate.

Ultimately, the airport would like to install a set of video analytics servers, each with unique purposes and capabilities. Content from these servers would be processed through an event correlation engine to identify and merge relevant data. This function is critical to eliminating unnecessary data collection and storage. The data would then be presented to security personnel who could use it to initiate timely actions and decisions.

By combining IP cameras and network-centric digital video management with video analytics software across a network, San Diego International Airport hopes to significantly improve its ability to detect intrusions, unauthorized entries and potential threats to civil aviation. In doing so, it will shift detection reliance from humans to technology, an innovative approach in airport security. Immediately and automatically detecting security anomalies and relaying critical, time-sensitive information and data to law enforcement and security personnel are vital initiatives in the mission to secure our nation's airports and air transportation system. STD

Mark Denari *is director of aviation security and public safety at the San Diego County Regional Airport Authority, where he directs, manages and administrates the airport's security and emergency/crisis preparedness programs. He also ensures that the airport complies with federally regulated standards.*

Dr. Dennis Charlebois *is director of product marketing in the Cisco physical security business unit.*

Security Leadership Solutions
Executive Council

Airports Encouraged to Use E-Verify

By Marleah Blades

On December 17, the Transportation Security Administration sent airport operators a memo asking them to recommend airport employers make the following items a security priority in 2008 (http://www.aaae.org/government/150_Transportation_Security_Policy):

- immediately notifying airport of change in employment status;
- reporting lost or stolen identification or access media and using such media appropriate1y;
- retrieving and returning such media of persons who no longer need them;
- conducting substantial identification verification processes;
- maintaining a high level of identification display and challenge; and
- preventing "piggybacking."

The memo's focus after this point is a recommendation for all airport employers to participate in the government's E-Verify program, previously known as the Basic Pilot/Employment Eligibility Verification Program. E-Verify is a free online program run by the Department of Homeland Security and the Social Security Administration that lets employers electronically verify the employment eligibility of newly hired employees.

Use of E-Verify is currently voluntary, but Congress is considering a bill that would make it mandatory for all U.S. employers, and Arizona's Legal Arizona Workers Act, which went into effect last month, requires Arizona employers to use the system. The federal government announced last summer that it would require all new federal contractors to enroll in and use E-Verify. Meanwhile, several organizations have raised their own concerns about the implications of nationwide mandatory use, such as privacy violations, network security and backlog.

Immigration reform is a huge issue in the campaigns for presidential nominations, and Americans are being bombarded with politically motivated messages for and against measures like mandatory use of E-Verify. The security picture is more nuanced than the ads make it sound. While few illegal workers pose a direct security threat to U.S. businesses, the potential does exist for terrorists to enter the country illegally with the intention of gaining access to airports.

According to Dennis Treece, director of corporate security for the Massachusetts Port Authority: "The E-Verify program can provide an increased level of security by verifying the basic credentials upon which employment is based. With identity theft becoming a national epidemic, we need tools to help us verify that people in whom we are putting considerable trust, and granting considerable responsibility and authority, are in fact who they say they are."

Airport operators and employers should consider the security pros and cons of using E-Verify while it remains a voluntary-use program. They should familiarize themselves with its operation enough to voice their support of or concerns about it to Congress as it considers requiring the program's use.

Marleah Blades is senior editor for the Security Executive Council, an international professional membership organization for leading senior security executives spanning all industries, both the public and private sectors, and the globe. The Security Executive Council maintains a large and growing list of laws, regulations, standards and guidelines that impact security (https://www.securityexecutivecouncil.com/public/lrvc). Visit www.SecurityExecutiveCouncil.com/?sourceCode=std for more information.