By John Purnell, *Inspired Data Solutions*

TWIC REVISITED

A consultant asks: Can it get its airport credentials back? The answer is 'yes'

The Transportation Worker Identification Credential (TWIC) was dismissed by the aviation community, but there is a way to make it work effectively for both the industry and government. Here is a proposed business model in which aviation and government can cooperate to achieve reduced operating costs and enhanced security. It's based on a reconsideration of TWIC and its role in the aviation community, and relates to recent Transportation Security Administration (TSA) initiatives such as the Aviation Credential Interoperable Solution (ACIS).

First, a review of what TWIC was originally intended to be and why the aviation community shunned it.

We begin with the successful Common Access Card (CAC) implemented throughout the Department of Defense (DOD) around the turn of the millennium. At about that time, the Universal Access Card, endorsed by the airline crews for common credentialing, had pretty much breathed its last.

The newly minted Transportation Security Administration (TSA) was also looking for a common credential that it could use in its domain. Every transportation employee would be issued a badge whose form, fit, and function would be dictated by the federal government. Mode by mode, the response to this program varied. In shipping ports and rail yards, TWIC promised to authenticate itinerant truck drivers where no existing credentialing alternative presented itself.

At airports, however, the response was chilly. As an industry, access control security was very mature, including a healthy partnership with FAA on setting standards. The access control systems (ACS) were installed and the processes for badge issuance and revocation well understood — and operational. Further, on the heels of the Screening System and Checkpoint deployment projects, the industry had more than its fill of federal mandates.

The aviation rebuttal focused on two points:

• There was already an extensive ACS infrastructure, and no money on either side of the debate to retrofit several hundred thousand door readers and several hundred ACS head ends.

• Second, airports have a wide variety of credential layouts which, by agreement with the feds, were changed when unaccounted credentials reached a certain limit. So, it was not possible for all airports to use a common access card, such as TWIC.

A NEED FOR CROSS-CREDENTIALING

In the first half of this decade we sorted out checkpoints, baggage systems, fingerprinting all employees, and a host of other aviation security issues. Amid that frenzy, a basic concept was never fully discussed by both sides of the TWIC debate. The simple point was that TWIC does not need to replace airport badges, but it can facilitate cross-credentialing.

Cross-credentialing is the acceptance of one party's successful adjudication by another party which has similar credentialing responsibilities. It is not common credentialing, such as the DOD CAC card, but it can be an effective alternative.

Many types of airport workers are credentialed at more than one airport. As airport and transportation consultants, many of us have had a full 'ten-print' taken several times each year. In my case, it has been seven in the last 24 months. At least five of these were processed by the same clearinghouse, analyzed by the same federal agency, and checked in the same criminal records database.

This multiple credentialing requires that employees that cross-credential carry a variety of documents with them all the time — passport, driver's license, even social security cards and/or birth certificates. There's a tremendous security risk in carrying all of this critical documentation all the time.

But consultants are not the only community to benefit from cross-credentialing. Air crews have long been interested in airport access at multiple airports. The Universal Access Card was their attempt to gain a single credential. Many have endured the tedious process necessary to obtain multiple airport badges. Maintenance workers often are credentialed at multiple airports. More than one company has expressed frustration that new employees spend the first three weeks of their employment getting credentialed at the multiple airports they will need to serve. The cost
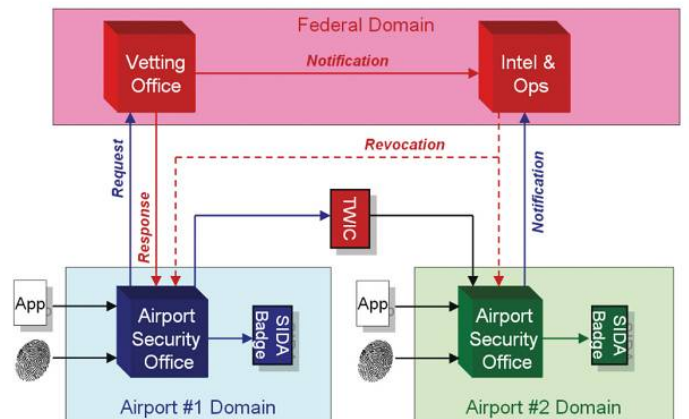
Use of TWIC for cross-credentialling can provide a comprehensive flow through the vetting process.

to industry and the aggravation to individuals caused by this inefficiency should be blatantly apparent.

TSA IS IN MOTION

According to Airports Council International-North America, TSA is "asking airports to provide a list of SIDA badge holders, sorted by company, that would also contain badge holder name, their employer, and badge expiration date." Presumably, this is in preparation for the Aviation Credential Interoperable Solution (ACIS).

Is ACIS really TWIC with a new name? Or perhaps the Air Line Pilots Association (ALPA) and TSA have joined up to resuscitate the Universal Access Card? Alternatively, this may be TSA repeating its mistakes of the past — trying to effect wholesale interoperability and biometrics at airports.

Whatever TSA's motivation for the change, the airport community may have an opportunity to interact in the formation of ACIS and prevent creation of another unilateral TWIC.

TWIC (OR ACIS) AS THE CROSS-CREDENTIAL

A federally issued identification card can, and should, be used to enable interoperation at airports. That does not mean that we should have only one credential. It is all right for airports to issue credentials for their premises. But a federal card such as TWIC or ACIS can be used to accelerate badge issuance while maintaining security. Should an employee wish to get a badge at another airport, he or she need only present the TWIC and verify their biometrics to receive a badge at the new airport. No second trip through the clearinghouse is needed.

A small amount of data integration will need to be organized by TSA. This would include:

• a means for an airport security office to securely verify that a TWIC card is currently valid and notify TSA that it has issued a credential based on TWIC;

• a means for TSA to issue revocation of a TWIC card to all airports that use that card as a cross-credential.

These simple, secure data exchanges are not difficult to implement and would have significant industry benefits.

ADDING UP THE BENEFITS

Everyone wins with TWIC as a cross-credential. Let's apportion the benefits out by stakeholder:

The Airport. The workload in the Security Office is reduced because TWIC holders get their badge in one visit, not two. Airport security is enhanced by having a better national revocation system and verification of an employee's history at other airports. Airports get to keep their current badges, policies, and access control systems.

The Employee. Getting a badge in one trip instead of two would be a huge benefit to employees; the inconvenience would be cut in half and work hours lost would be significantly reduced. In the case of lost or stolen credentials, authentication using TWIC biometrics should speed up the issuance of a new badge, meaning less time off the job.

The Employer. The cost of getting badges is usually felt by the employer, be it the airport or an airport-based busi-

ness. Costs would drop because employees spend less time getting badges, and pay less (or nothing) for badges at the second, third, and fourth airports.

The TSA. The government gets national revocation capability and better assurance that an employee at airport 'A' is the same individual as the employee at airport 'B'.

TSA also gets a new mode for TWIC, which may prove useful when a TWIC-carrying trucker shows up to drop a load at the airport instead of the rail yard or ocean port. And, TSA can get a population of users with ACIS or TWIC cards in hand. When an airport goes to implement biometric-based access control, it can choose an ACIS-compatible system if it wishes to use the federal card

as its SIDA badge. This is an evolutionary approach to achieving SIDA II.
* * *
This is one of those situations where everyone needs to take a step back for the good of the industry. TSA needs to back off of the notion that it will take over the form and function of all SIDA credentials. Airports need to work with TSA to achieve national revocation and biometric-based identity management. Employers and employees must work within the system rather than reinventing the system. Over time, Darwinian natural selection will show us how these conflicting goals are best achieved. In that context, maybe ACIS, the cross-credential, is our next evolutionary development.

About the Author

John Purnell is an airport and transportation consultant, providing clients with strategic application of information technology and security systems. He has some 30 years aviation experience, and is based in Annapolis, MD. Reach him at John.Purnell@InspiredDataSolutions.com.

How TSA Defines TWIC for Ports

TSA's website (www.tsa.gov) outlines the Transportation Worker Identification Credential as follows for U.S. ports:

"TWICs are tamper-resistant biometric credentials for workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities, and all credentialed merchant mariners. It is anticipated that more than 750,000 workers including longshoremen, truckers, port employees, and others will be required to obtain a TWIC.

"To obtain a TWIC, an individual must provide biographic and biometric information such as fingerprints, sit for a digital photograph and successfully pass a security threat assessment conducted by TSA.

"Workers can avoid lines and save time during the process by pre-enrolling online (pre-enrollment began October 9, 2007). Here workers provide biographical information and make a reservation to complete the process in person at the port."