

BEST PRACTICES FOR AIRPORT BADGE OFFICES TO COUNTER FRAUDULENT DOCUMENTS

(8/20/2012)

This summary is provided for circulation on the Airport Web Board by the Transportation Security Administration, Office of Security Policy and Industry Engagement (OSPIE), Aviation Division Airports Branch. The TSA does not endorse any specific practice but rather offers this information to airport operators should it be of interest. This listing is provided in the interest of information exchange to enhance procedures to counter fraudulent document use in the airport badge application process. The U.S. Government assumes no liability for the contents or use. This listing does not create regulatory requirements or mandates of any kind. There are recommendations contained in this list that may prove beneficial in some airport badge issue office environments but not in others. This summary is divided into six main areas which include training, software use, web based tools, hardware, documents, and procedures. This summary is by no means complete but offers some reasonable solutions for consideration to counter fraudulent document use.

Training: In the training area: in an effort to highlight best practices for airport badge offices to consider and implement, OSPIE has partnered with the Customs Border Protection (CBP) Office for Fraudulent Documents to put together a ninety minute training session to be conducted by CBP officers at the twenty regional areas that are supported by CBP port directors. This coincides by and large with Category X airport locations. The Federal Security Director (FSD) at each Category X or his designated representative will be the coordinator for scheduling the training with the local airport operator staff. The target for the training is the airport badge office staff. CBP Fraudulent Documents Center has been provided contact information for all Category X FSD's and will conduct reach out to start the process. In order to maximize these training events, FSD's have been asked to reach out to their spoke airports to have representatives sit in on the training conducted at the Category X airports.

Software: Posted on this web board as a standalone section is a listing of Best Practices for Automated Badge Issue techniques.

Web Based: Some web based tools are offered for badge office consideration: SSN.Validator.com, driverslicenseguide.com, and Docutector.com.

Hardware: Hardware in the form of document scanners that have been found to be useful in document verification includes and is not limited to: Border Guard, iA-Authenticate B5000, and QC-1.

Publications: US Immigration and Customs Enforcement (ICE) Publication M-396 posted separately in entirety on this web board and Pocket Guide Reference to Document Security Features and Printing Techniques published by ICE Forensic Document Laboratory. Copies of the latter document will be provided to CAT X Federal Security Directors for distribution in the near future.

Procedures: Two procedures are shared that are currently in use at some airports:

- Annual badge renewal vice two years
- First time badge issue to expire in six months (counters early employee attrition)