Controls Over Airport Identification Media
Federal Aviation Administration

Report Number AV-2001-010 **December 7, 2000**

The Office of Inspector General has issued an audit report on Controls Over Airport Identification Media. Controlling access to secure airport areas has been, and continues to be, an area of great concern due to increased threat to U.S. airport facilities. Two important access control requirements are to limit access to secure airport areas to only individuals who can be trusted with the public's safety and immediately deny access when an individual's authority changes. FAA has not taken adequate steps to ensure these requirements are met. Specifically:

- FAA's background investigation requirements for issuing airport identification media (airport ID[1]) are ineffective because they do not accomplish their intended purpose of providing adequate assurance that individuals who are granted unescorted access to secure airport areas can be trusted with the public's safety. For example, Federal Bureau of Investigations criminal record checks (criminal checks) are only required for individuals applying for airport ID when one of four conditions triggers the checks. One of the triggers, a 12-month unexplained gap in employment, was designed to identify individuals who were incarcerated for committing a serious crime. However, we found that the trigger is ineffective because not all individuals convicted of serious crimes have a 12-month gap in employment.

  FAA must issue new rules to strengthen its background investigation requirements and include initial and randomly recurring criminal checks for all employees. On November 22, 2000, the President signed the Airport Security Improvement Act of 2000 (Public Law 106-528), which will strengthen background investigation requirements. FAA and the airport industry have stated support for the legislation. To further help determine the trustworthiness of employees, FAA should consider using other investigative tools, such as credit checks and drug tests, to determine whether individuals are trustworthy.

- Until new rules can be established, industry must comply with existing requirements. However, we determined that background investigation requirements were frequently not followed by airport operators, air carriers and airport users. For 35 percent of the employees randomly

Airport users include foreign air carriers, non-air-carrier airport tenants, and companies that do not have offices at the airport, but require access to the airport's secure area.

[1] OIG defines **"airport ID"** as all media issued to individuals to permit unescorted access to secure areas.

selected for review at six airports, we found no evidence (19 percent) or incomplete evidence (16 percent) that background investigations were performed as required. In addition, recent investigations resulted in fining two companies doing business at major U.S. airports for falsely certifying that background investigations were performed when, in fact, they were not.

- Until the background investigation regulations are changed, FAA needs to ensure industry's compliance with requirements. We found that FAA's oversight of air carriers' and airport users' compliance with current regulations needs improvement. For example, FAA's previous national assessments of compliance mainly focused on airport users at 20 major U.S. airports, and for the airports we reviewed, the actions taken by FAA to correct the deficiencies identified during the assessments were not always effective.

- Also, FAA should issue a planned revision to regulations, which will require airport operators and air carriers to audit the number of active airport IDs at least once a year. FAA must also issue standard audit procedures to ensure these audits are effective. We determined that airport operators had not developed and implemented adequate procedures to account for airport ID and immediately deny access to secure airport areas when required. At the 6 airports reviewed, we found that 9 percent (234 of 2,586 reviewed) of the IDs issued for access to secure airport areas remained active, even though the employee's authority had changed and access was no longer required.

The FAA has determined the report contains some sensitive security information. Therefore, the report will not be placed on our website; however, FAA will have a redacted version of this report available. If you want a copy of the report, please call Rebecca Trexler, FAA Public Affairs, at (202) 267-8521.