

November 25, 2002

Federal Aviation Administration
Docket Management System
Attention: Docket No. FAA-2002-11666
U.S Department of Transportation
400 Seventh Street SW
Room 401, Plaza Level
Washington, DC 20590-0001

Gentlemen and Ladies:

Thank you for the opportunity to comment on Final Rule 61.3(a) and 61.3(1) whereby each person must carry a photo identification acceptable to the Administrator when exercising the privileges of a pilot certificate and present such photo identification when requested to do so by authorized personnel.

Imaging Automation is a leader in document authentication equipment and has years of experience authenticating passports worldwide and, more recently, US drivers licenses. It is our belief, based on experience, that presenting a photo ID offers no additional security unless the ID has embedded security features and equipment is available to detect the presence or absence of these security features.

Currently, drivers licenses rarely contain security features and their production and design is not standardized within the US. It is well-known that drivers licenses are easily forged. A few states still do not provide a photo on their drivers licenses and several provide neither magnetic stripe nor bar code formatting. The more determined the perpetrator, a terrorist for example, the more likely the forgery is to be of very high quality. High-quality forgeries are undetectable by a visual inspection.

Passports, on the other hand, especially those meeting ICAO standards such as the US passport, are produced at regional printing centers under strict quality control. They contain embedded security features and there is standardization within each series. Passport forging is much more difficult to do well and is more easily detected with equipment like Imaging Automation's iA-thenticate platform which is trained to look for known forgery techniques. Most pilots already have a valid passport.

Imaging Automation recommends a "layered" approach to security. The iA-thenticate platform is available now to authenticate machine-readable documents, such as passports, as well as US and Canadian drivers licenses. Software packages like iA-Passport, DL Alert and On-line Verification enable the iA-thenticate platform to authenticate at various levels. iA-thenticate supports several biometric tools and can scan Watch Lists. Security will be increased immediately yet the robustness of the technology allows the FAA to meet future identification requirements.

We encourage the FAA to consider using passports now as a short-term solution to increase security. We also recommend implementing a layered approach to security to decrease the likelihood of non-authorized individuals gaining access to aircraft. Imaging Automation would like to make its expertise available to the FAA in this effort.

Sincerely,

Rick Carter, Sr. Sales Director
Travel and Transportation