STATEMENT OF MARGARET GILLIGAN, ASSOCIATE ADMINISTRATOR FOR AVIATION SAFETY, FEDERAL AVIATION ADMINISTRATION, BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON TRANSPORTATION AND PUBLIC ASSETS, ON "SECURING OUR SKIES: OVERSIGHT OF AVIATION CREDENTIALS," February 3, 2016.

Chairman Mica, Ranking Member Duckworth, Members of the Subcommittee:

Thank you for the opportunity to appear before you today on the issue of oversight of aviation credentials. I know that this issue has been and continues to be of significant interest to Chairman Mica. The Federal Aviation Administration (FAA) previously appeared on this issue before the Subcommittee on Government Operations in 2013 and before the Committee on Transportation and Infrastructure in 2011, both under Chairman Mica's leadership.

FAA continues to support the Transportation Security Administration (TSA) and other security and intelligence agencies to keep our skies secure. FAA is mindful of the risks identified by our security partners and has taken steps to close security gaps as advised by these agencies.

The FAA issues 23 different types of airman certificates, held by mechanics, dispatchers, parachute riggers, and air traffic controllers, in addition to the 6 types held by pilots. Active pilot certificate holders number approximately 861,000. Historically, a pilot certificate was evidence that the pilot was trained and competent to conduct the operations authorized by the certificate. The certificates, used for decades, worked effectively for this intended purpose.

As other agencies with mandates other than aviation safety began to see potential misuse of pilot certificates, FAA took steps to enhance the security of all airman certificates. Pursuant to the

Drug Enforcement Administration (DEA) Act of 1988, for example, the agency phased out paper certificates and replaced them with plastic certificates that incorporate tamper- and counterfeit-resistant features including micro printing, a hologram, and a UV-sensitive layer.

Since 2002, the FAA has required a pilot to carry a valid Government issued photo I.D. in addition to a pilot certificate while exercising the privileges associated with the certificate. This allows an FAA inspector, or a fixed base operator who rents airplanes, to confirm both the pilot's identity and his or her pilot qualifications.

Each time a pilot applies for a certificate or rating, the applicant is required to present an acceptable form of photo identification to the FAA inspector or designee. Acceptable forms of identification include a driver's license issued by a State, the District of Columbia, or a territory or possession of the United States; a Government issued identification card; or a passport. In addition to a photo, the identification must include the applicant's signature and residential address, if different from the applicant's mailing address. This information may be presented in more than one form of identification, and special procedures exist to verify the identity of applicants who do not possess suitable forms of identification, such as minors. We allow these alternatives because a pilot certificate does not impart security access privileges and the intended purpose of the certificate is not for use as an identification media or security credential, but simply to affirm a pilot's qualification.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) imposed additional requirements for pilot certificates, including that they be tamper-resistant and include a photograph of the pilot. The certificates were also required to be capable of accommodating a

biometric identifier, such as a digital photo or fingerprint, or any other unique identifier FAA deemed necessary.

FAA met some of these requirements when it began issuing tamper- and counterfeit-resistant plastic certificates in 2003. In response to the remaining requirements of IRTPA, the FAA issued a Notice of Proposed Rulemaking (NPRM) in 2012 to require a photo of the pilot on all plastic pilot certificates, and student pilots to apply for, obtain, and carry plastic certificates while exercising the privileges of the student pilot certificate. While the agency was reviewing the hundreds of comments received on the NPRM, the FAA Modernization and Reform Act of 2012 became law. Section 321 of that Act required that pilot certificates not only contain photographs, but also be smart cards that can accommodate iris and fingerprint biometric identifiers and comply with FIPS-201 or Personal Identity Verification-Interoperability Standards (PIV-1) for processing through security checkpoints into airport sterile areas. The FAA's 2012 NPRM did not contemplate those additional features.

Upon further review of the NPRM, the security and intelligence communities identified a security gap in FAA's process for issuing student pilot certificates. With respect to this population, applicants could be issued a student pilot certificate before TSA had vetted the applicants. In 2012, the agency shifted its focus to closing the security gap in student pilot vetting. On January 12 of this year, the FAA published a final rule requiring student pilots to apply for a plastic certificate by appearing in person at a Flight Standards District Office (FSDO) or before a designated pilot examiner, an airman certificate representative associated with a flight school, or a certified flight instructor. These authorized individuals will be able to accept a student pilot application and verify the applicant's identity, but will not be able to issue a student

pilot certificate. The Civil Aviation Registry, located in Oklahoma City, Oklahoma, will provide the applicant's information to TSA for vetting before the certificate is issued. The Civil Aviation Registry will issue a permanent student pilot certificate only after receiving a positive response from TSA.

In 2013, we prepared and submitted a report to Congress on Section 321. As discussed in our report, an initial estimate of the cost of the transition to an enhanced pilot certificate is approximately $1.125 billion over 12 years.

Given the substantial cost to pilots and taxpayers, we must coordinate with the Department of Homeland Security (DHS) and TSA to carefully consider the benefits of enhanced pilot certificates. If pilot certificates with embedded biometrics are intended to permit airport access or increase security, hundreds of airport access control systems would have to be created or retrofitted to ensure consistent use and verification of the biometrics.

In this regard, the National Institute of Standards and Technology (NIST) has developed standards defining how to collect iris biometric data. Now other government agencies, however, will need to develop the infrastructure to utilize this information. Understanding how best to use biometric data to enhance the security of the pilot community and aviation security overall will require continued coordination among government agencies in cooperation with airlines, airports, aviation labor groups, and others. FAA must also be mindful of the costs and benefits of these security enhancements as it evaluates the feasibility of a rule that can meet statutory mandates and accommodate rapidly evolving technologies.

We look forward to working with you, in collaboration with other agencies, and the aviation industry.