STATEMENT OF JOHN ALLEN, DIRECTOR OF FLIGHT STANDARDS SERVICE, FEDERAL AVIATION ADMINISTRATION, BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON GOVERNMENT OPERATIONS, ON THE INCLUSION OF BIOMETRIC IDENTIFIERS ON GOVERNMENT ID CARDS, June 19, 2013.

Chairman Mica, Congressman Connolly, Members of the Subcommittee:

Thank you for the opportunity to appear before you today on the issue of incorporating biometric data into pilot certificates. I know this issue has been of significant interest to Chairman Mica. The FAA previously appeared before the House Committee on Transportation and Infrastructure on this issue under Chairman Mica's leadership in 2011.

The FAA has responsibility for issuance of 23 different types of airman certificates. In addition to pilot certificates, these include certificates for mechanics, dispatchers, parachute riggers, and air traffic controllers. The agency also issues certificates to flight attendants. There are approximately 837,000 active pilot certificate holders.

Historically, the primary function of a pilot certificate was simply to document that its holder meets the aeronautical knowledge and experience standards established for both the certificate level and any associated ratings.

Even before the September 11 terrorist attacks, the FAA was responding to law enforcement interest in enhancing the security of airman certificates. Pursuant to the Drug Enforcement Administration (DEA) Act of 1988, for example, the agency began the process of phasing out paper certificates and replacing them with plastic. Since April 2010, all pilots have been required to have the new plastic certificates. Holders of the remaining airman certificate types –

that is, navigators, mechanics, dispatchers, etc. – were required to have a security-enhanced plastic certificate by March 31, 2013. As of March 31, all airman certificate holders, including pilots, have plastic certificates that incorporate tamper- and counterfeit-resistant features. These include micro printing, a hologram, and a UV-sensitive layer.

As you know, the Intelligence Reform and Terrorism Prevention Act (IRTPA) that the Congress passed in 2004 requires additional security measures for pilot certificates. Specifically, the IRTPA directed the FAA to develop tamper-resistant pilot certificates that include a photograph of the pilot and are capable of accommodating a digital photograph, a biometric identifier, or any other unique identifier the FAA Administrator considers necessary.

The FAA had already met some of these requirements when it began issuing tamper- and counterfeit-resistant certificates in 2003. To address the remaining requirements, the FAA was required to initiate a rulemaking. Before I discuss the rulemaking effort, let me note that the FAA chose to use a digital photo as the method of complying with IRTPA. However, we are working closely with the Transportation Security Administration (TSA) on measures that will provide additional security enhancements not only to pilot certificates, but also to other types of airman certificates.

The FAA has also taken other steps to meet law enforcement concerns. Since 2002, the FAA has required pilots to carry a valid Government issued photo ID as well as a pilot certificate in order to exercise the privileges associated with the certificate. This allows an FAA inspector or a

fixed-base operator that rents airplanes to confirm both the individual's identity and his or her pilot credentials.

In response to IRPTA, the FAA initiated a rulemaking to require digital photographs to appear on pilot certificates. While the agency was reviewing the hundreds of comments received on the Notice of Proposed Rulemaking (NPRM) the FAA Modernization and Reform Act of 2012 became law. Section 321 of that Act requires that pilot certificates not only contain photographs, but also be smart cards that can accommodate iris and fingerprint biometric identifiers and are compliant with FIPS-201 or Personal Identity Verification-Interoperability Standards (PIV-I) for processing through security checkpoints into airport sterile areas. The FAA's NPRM did not contemplate those additional features.

Because the requirements of Section 321 were not within the scope of the previous NPRM, the agency was required to initiate another rulemaking in order to comply with congressional directives. The rulemaking process requires the FAA to propose requirements for an applicant to obtain and use an improved pilot certificate, analyze the costs and benefits of those requirements, consider public comments to the proposal, and issue final requirements. In accordance with this process, the FAA is developing a notice of proposed rulemaking to issue smart card pilot certificates that can accommodate a photograph and other biometric data.

The cost of this transition has not yet been determined, but analysis of the costs and benefits of various alternatives to meet the statutory mandate is underway.

To justify imposing a new cost on pilots, we must carefully consider the benefits of improved pilot certificates. If pilot certificates with embedded biometrics are intended to permit airport access or increase security, we must coordinate with the Department of Homeland Security (DHS) and the TSA, which develop standards for airport access and security.

There are also implications for multiple government agencies. The National Institute of Standards and Technology (NIST) is in the process of a rulemaking that will establish standards to enable the use of iris biometric data, but has not yet established this standard. That impacts the FAA, since the agency seeks to avoid duplicating, interfering with, or superseding efforts by other federal agencies with respect to standards or implementation. To address and coordinate these issues, and to evaluate quantifiable benefits regarding how this technology might advance each agency's mission, the FAA is participating in an interagency working group that includes DHS through the TSA, as well as NIST. In addition to avoiding duplication or conflicting standards that would impose an undue burden on pilots, the working group seeks to learn from best practices in other agencies. One such example is the DHS Global Online Enrollment System (GOES) for managing the U.S. government's trusted traveler programs.

It is therefore essential to identify and quantify the benefits of biometric enhancements as we move forward.

Understanding how to maximize the use of biometric data to ensure the security of the pilot community, to enhance overall aviation security in a way that does not create duplication or impose an undue burden, and to craft a rule that can meet the statutory mandates, while

accommodating rapidly evolving technologies. It will also require a government working group (through FAA's Aviation Rulemaking Committee process) to coordinate with airlines, industry trade associations, and organizations representing individual pilots.

We are working hard to accomplish the goals outlined by Congress. In consultation with other agencies, the FAA is in the final stages of preparing a report to Congress. We believe this report will assist Congress in assessing the future use and inclusion of biometric data in pilot certificates. We look forward to working with you, and in collaboration with other agencies, as our efforts progress.

This concludes my prepared remarks. I will be happy to take questions at this time.

John M. Allen
Director, Flight Standards Service
Federal Aviation Administration

John Allen joined the Federal Aviation Administration in November 1991 and was appointed as the Director, Flight Standards Service in December 2008. He leads an organization of more than 4800 aviation professionals responsible for promoting the safety of Flight for civil aircraft by setting regulations and standards for air carriers, air agencies, general aviation, airmen, and designees. Flight Standards also is responsible for the certification, inspection, surveillance, investigation, and enforcement of aviation regulations. The organization manages the aircraft and airmen official registry system.

Before his appointment as the Director, Mr. Allen served as the Deputy Director beginning in March 2003, and as Assistant Manager, Flight Standards Certification and Surveillance Division (AFS-900) at Dulles International Airport, beginning in December 1998. In his capacity as Assistant Division Manager, he assisted the Division Manager with leading 150 employees in the system safety-based certification and oversight of air carrier certificate holders. AFS-900 was responsible for the management of the Air Transportation Oversight System (ATOS), the Certification, Standardization, and Evaluation Team (CSET) and the Flight Standards Safety Analysis Information Center (FSAIC).

Prior to AFS-900, Mr. Allen served in the Advanced Qualification Program Branch (AFS-230) as an Aviation Safety Inspector (Operations). As an AQP ASI, he assisted the Certificate Management Offices (CMO) and flight training departments of Northwest Airlines, US Airways, Trans World Airways, Delta Airlines and other airlines with the initiation of “Single-Visit” training and their Advanced Qualification Programs

Mr. Allen retired as a Brigadier General from the Air Force Reserves in 2009. He held various command positions during his 31-year active duty and reserve military career, to include vice wing commander and squadron commander.

He has over 4,800 flying hours; most of it obtained as an instructor and examiner pilot on the military C-141 for 20 years and as an Air Force instructor pilot in the T-37. He has an Air Transport Pilot (ATP) certificate with ratings in the A-320 and L-300 (C-141).

Mr. Allen received his Bachelor of Science degree in computer and information sciences from the University of Florida. He also received a Master of Science degree in aeronautical technology from Arizona State University.

He is married and has two sons. Hobbies include golf, flying, sailing and scuba diving.