U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

December 10, 2013

The Honorable John D. Rockefeller, IV
Chairman, Committee on Commerce,
Science, and Transportation
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

As required in Section 321 of Public Law (PL) 112-95, FAA Modernization and Reform Act of 2012, I am pleased to provide you with the report to Congress on improved pilot licenses.

We have sent identical letters to Chairman Shuster, Senator Thune, and Congressman Rahall.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

December 10, 2013

The Honorable John Thune
Committee on Commerce,
Science, and Transportation
United States Senate
Washington, DC 20510

Dear Senator Thune:

As required in Section 321 of Public Law (PL) 112-95, FAA Modernization and Reform Act of 2012, I am pleased to provide you with the report to Congress on improved pilot licenses.

We have sent identical letters to Chairmen Shuster and Rockefeller, and Congressman Rahall.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

December 10, 2013

The Honorable Bill Shuster
Chairman, Committee on
Transportation and Infrastructure
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

As required in Section 321 of Public Law (PL) 112-95, FAA Modernization and Reform Act of 2012, I am pleased to provide you with the report to Congress on improved pilot licenses.

We have sent identical letters to Chairman Rockefeller, Senator Thune, and Congressman Rahall.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

U.S. Department
of Transportation

**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., S.W.
Washington, D.C. 20591

December 10, 2013

The Honorable Nick J. Rahall, II
Committee on Transportation and Infrastructure
House of Representatives
Washington, DC 20515

Dear Congressman Rahall:

As required in Section 321 of Public Law (PL) 112-95, FAA Modernization and Reform Act of 2012, I am pleased to provide you with the report to Congress on improved pilot licenses.

We have sent identical letters to Chairmen Shuster and Rockefeller, and Senator Thune.

Sincerely,

Michael P. Huerta
Administrator

Enclosure

Table of Contents Page

1.0 Executive Summary

This report responds to Section 321 of Public Law 112-95, the FAA Modernization and Reform Act of 2012, which required the FAA to provide a report containing a timeline for the phased issuance of improved pilot licenses (certificates) that ensures all pilots are issued such licenses (certificates) no later than two years after the initial issuance of the improved pilot licenses (certificates). The Act describes the requirements for the improved pilot licenses, which are discussed later in this report. The Act further directs that this report include recommendations for the Federal installation of infrastructure necessary to take advantage of information contained on improved pilot certificates issued; identify the Federal entity that should be responsible for installing, funding, and operating the infrastructure at airport sterile areas; and provide an estimate of the costs of the infrastructure.

The FAA formed an Improved Pilot Certificates working group to respond to Section 321. The working group consists of multiple FAA offices, as well as the Transportation Security Administration (TSA). The working group examined the FAA's current certification processes and explored other pilot certificate options that would meet the requirements as set forth by Congress. The working group continues to discuss the infrastructure necessary to take advantage of information contained on improved pilot certificates. The TSA provided the FAA with input in regard to TSA's operational concerns on the security infrastructure at the nation's airports because the FAA does not currently have any infrastructure in place to capture biometrics for pilots or a means to take advantage of pilot certificates that would contain biometric information. The TSA does not fund airport security measures related to pilot access controls (biometric capture, etc.). Rather, airport infrastructure improvements are funded through a combination of revenue generated from an airport's operations, funding from State and local governments, and FAA grants.

This report discusses various aspects of the current pilot certificate and infrastructure that are in place. The report also examines the various smart card aspects for the improved pilot certificate. Prior to issuing improved pilot certificates, the FAA must initiate rulemaking to exercise the statutory authority for collecting the required biometric data and associated fees. The FAA must provide the public with an explanation of the requirements for submitting biometrics, obtaining and using improved pilot certificates, as well as estimated costs and benefits of the requirements in the notice of proposed rulemaking (NPRM) and final rule. Prior to issuing a final rule, the FAA must consider all substantive comments to the proposal. This report provides a preliminary estimate of costs associated with the FAA and individual pilots for the issuance of improved pilot certificates. As the FAA proceeds with rulemaking and performs more detailed analysis, these estimates may change.

2.0 Legislative Mandate

Public Law 112-95, Section 321 (reference Appendix 1 of this report) further directs the FAA to issue improved pilot certificates consistent with certain requirements. The improved pilot certificates must be compliant with Federal Information Processing Standards-201-1 (FIPS 201-1) or Personal Identity Verification – Interoperability Standards (PIV-I) for processing through security checkpoints into airport sterile areas. The certificates must be resistant to tampering, alteration, and counterfeiting; must include a photograph of the individual to whom the certificate is issued for identification purposes; and must be a smart card, which is able to accommodate iris and fingerprint biometric identifiers.

Section 321 directs the FAA to provide this report to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate. This report contains a timeline for the phased issuance of improved pilot certificates with biometrics that ensures all pilots are issued such certificates not later than two years after the initial issuance of the improved pilot certificates. This report also identifies the need for the Federal installation of infrastructure necessary to take advantage of information contained on improved pilot certificates issued; identifies the Federal entity that should be responsible for installing, funding, and operating the infrastructure at airport sterile areas; and provides an estimate of the costs of the infrastructure.

3.0 Background

3.1 FAA Issuance of Airman Certificates and International Compliance

The FAA issues certificates to pilots under the authority granted in Title 49 of the United States Code (U.S.C.), Chapter 447, Section 44703, which delegates the issuance of airman certificates to the FAA Administrator. Section 44703 permits modifications to the airman certification system to make the system more efficient in serving the needs of those enforcing laws related to the regulation of controlled substances and related to combating acts of terrorism by ensuring positive and verifiable identification of each individual applying for or holding a certificate. The FAA established regulations on how to obtain a pilot certificate, when a pilot certificate must accompany a pilot, and how the pilot certificate will be utilized. The applicable regulations include 14 CFR part 61, Certification: Pilots, Flight Instructors, and Ground Instructors; part 91, General Operating and Flight Rules; part 121, Operating Requirements: Domestic, Flag, and Supplemental Operations; part 125, Certification and Operations: Airplanes Having a Seating Capacity of 20 or More Passengers or a Maximum Payload of 6,000 Pounds or More; and Rules Governing Persons on Board Such Aircraft; part 135, Operating Requirements: Commuter and On Demand Operations and Rules Governing Persons on Board Such Aircraft; part 141, Pilot Schools; and part 142, Training Centers.

The FAA issues pilot certificates that also conform to standards set forth by the International Civil Aviation Organization (ICAO) in Annex 1: Personnel Licensing. ICAO is a specialized organization of the United Nations to promote the safe and orderly development of civil aviation throughout the world. It sets standards and recommendations necessary for aviation safety, security, efficiency and regularity, and environmental protection. ICAO serves as a forum for cooperation in all fields of civil aviation among the 191 Member States. If the U.S. did not conform to ICAO standards, other member countries of ICAO would be able to deny a U.S. aviation operation entry into that nation. The FAA will ensure that all pilot certificates issued by the U.S., including those mandated by Section 321 of Public Law 112-95, will continue to conform to 49 U.S.C. 44703 and ICAO standards.

3.2 Intended Purpose of a Pilot Certificate

Historically, the intended purpose of a pilot certificate is to display the level of the certificate, ratings, limitations, and operating privileges that a pilot has demonstrated and has been found to be competent to conduct specific aircraft operations. Each time a pilot makes application for a certificate, rating, or authorization, positive identification of the applicant is made by requiring a pilot to present an acceptable form of photo identification to an FAA Aviation Safety Inspector or Designated Pilot Examiner. The photo identification must be a driver's license issued by a State, the District of Columbia, or territory of the United States, a U.S. Government identification card, a U.S. Armed Forces identification card, or an official passport. An airman certificate does not impart security access privileges and the certificate's intended purpose has never been as a security credential. The FAA requires pilots to carry acceptable photo identification

when exercising privileges of the pilot certificate. A pilot may continue to exercise privileges of a certificate until the certificate is suspended, revoked, cancelled, or it becomes obsolete or is voluntarily surrendered. The pilot may also exercise the privileges of a Temporary Airman Certificate pending receipt of the permanent certificate. A Temporary Airman Certificate may be utilized by pilots, who are already known to the FAA, for a period of up to one hundred-twenty days unless superseded by the airman's permanent airman certificate.

3.3 Regulatory History

In the FAA Drug Enforcement Assistance Act of 1988 (DEA Act),[1] Congress identified deficiencies in the FAA's aircraft registration and pilot certification systems and required the FAA to correct them. As a result, the FAA published a Notice of Proposed Rulemaking (NPRM) to address the deficiencies but later withdrew it after determining that technological improvements could accomplish most requirements of the DEA Act. As part of the technological improvements, the FAA discontinued issuing paper pilot certificates and began issuing security-enhanced airman certificates in July 2003. The tamper and counterfeit-resistant certificates are made of high-quality plastic card stock and contain such features as micro printing, a hologram, and a UV-sensitive layer.

President George W. Bush signed the Intelligence Reform and Terrorism Prevention Act (IRTPA) in December 2004. Section 4022 of that law required the FAA to issue improved pilot certificates that (1) are resistant to tampering, altering, or counterfeiting; (2) include a photograph of the individual to whom the certificate is issued; and (3) 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 the IRTPA requirements when it began issuing tamper- and counterfeit-resistant certificates in 2003. To address the remaining requirements that could not be completed without rulemaking, the FAA published the Drug Enforcement Assistance NPRM (72 FR 489) in January 2007. The NPRM proposed changes to the airman certification and aircraft registration requirements to comply with the DEA Act. In February 2008, the FAA published the Drug Enforcement Assistance final rule (DEA final rule) (73 FR 10662). In that rule, the FAA required all pilots, except student pilots, to obtain a plastic certificate by March 31, 2010. After that date, pilots without plastic certificates could not exercise the privileges of their certificates. The FAA determined that the DEA final rule satisfied the IRTPA requirement to issue pilot certificates that are resistant to tampering, altering, and counterfeiting. The FAA continues to issue paper temporary pilot certificates and paper student pilot certificates.

On November 19, 2010, the FAA published an NPRM titled "Photo Requirements for Pilot Certificates" (75 FR 70871). The NPRM proposed to fulfill the final requirements of section 4022 of the IRTPA by requiring a photo of the pilot on all plastic pilot certificates, including student pilots. The FAA also proposed a $22 fee to process an application for (1) exchanging an existing certificate without a photo for a certificate with

[1] Public L. 100–690, 102 Stat. 4181 (Nov. 18, 1988).

a photo, (2) issuing a new pilot certificate or student pilot certificate with a photo, and (3) replacing a pilot certificate with a photo whenever a replacement certificate is requested by a pilot or required by regulation. The FAA proposed that pilots be required to update their photo every 8 years, similar to the Real ID Act of 2005 requirements. The FAA proposed a 5-year phased implementation period to minimize the burden of reissuance on pilots and the Agency as well as to help ensure that the FAA processes the pilot certificates with a photograph without delay for those who are employed in air transportation.

The FAA received approximately 470 comments from individual pilots, Transport Canada, and several aviation associations, which represent thousands of pilots. Most commenters opposed the concept of adding a photo to the pilot certificate, as well as the proposal to require student pilots to have a certificate with a photo. The FAA received comments on the following general areas of the proposal:

- Requirement of a photo on pilot certificates;
- Fees for obtaining new, replacement, or renewed pilot certificates with photo;
- Inclusion of students in the requirement to have certificates with photo;
- Duration of validity for the photo;
- Application process for new, replacement, or renewed pilot certificates with photo;
- Implementation process using "trigger" events and phased deadlines;
- Regulatory evaluation; and
- Lack of safety and security benefits.

The FAA believes that the 2010 NPRM addresses all requirements except Section 321(c)(3). That section requires that pilot certificates be smart cards that (a) accommodate iris and fingerprint biometric identifiers, and (b) are compliant with FIPS 201-1 or PIV-I for processing through security checkpoints into airport sterile areas. The FAA, in conjunction with an interagency working group, is in the process of evaluating this rulemaking project (and other rulemaking alternatives) in light of Section 321 requirements.

4.0 Current FAA Infrastructure Relating to Pilot Certification

Section 321 requires the FAA to make recommendations for the Federal installation of infrastructure necessary to take advantage of information contained on improved pilot certificates. In order to gain a complete understanding of the future infrastructure that must be identified, an overview of the FAA's current infrastructure and role is necessary. Recommendations follow in Section 8.0 below.

The FAA currently issues pilot certificates based on information submitted by a pilot applicant. Pilot applicants provide the FAA with their biographical and eligibility information using an FAA form at the time of application for a certificate or rating. The FAA form is submitted to an Aviation Safety Inspector or authorized designee of the FAA prior to certification. Applicants are not required to submit fingerprints or a photograph; however, pilots are required by FAA regulations to provide positive identification at the time of application for a certificate and must carry positive identification while exercising pilot privileges.

The FAA's Office of Aviation Safety, Flight Standards Service operates 90 facilities that are open to the public, by appointment, across the United States. These facilities, known as Flight Standards District Offices (FSDOs), are composed of inspectors who accept applications for pilot certificates and have authority to issue temporary pilot certificates to pilot applicants. The FAA also utilizes approximately 2,900 authorized designated examiners who perform certification activities and issue pilot certificates. These authorized designees accept applications and test the pilot's knowledge, skills, and abilities for the certificate, rating, or authorization the pilot is seeking. The application and supporting documents are submitted to FAA and processed by the FAA's Civil Aviation Registry, which reviews and records the documentation into the airman's official record and issues a permanent airman certificate. The Civil Aviation Registry also collects biographic data for FAA statistical and reporting purposes. In October 2007, the FAA entered into an agreement with TSA to provide the biographic airmen information to TSA for vetting against the consolidated Terrorist Screening Database (TSDB). On a daily basis, TSA adds new airmen in the Registry to its vetting system; on a weekly basis, TSA adds the records of airmen that have been updated or changed to its vetting system. All information in the TSA vetting system is then compared to the TSDB on a daily basis.

The Civil Aviation Registry is responsible for the issuance of the permanent airman certificate (except for student pilot certificates). Pilot certificates are issued without an expiration date and pilots may continue to exercise privileges unless the certificate is suspended or revoked, cancelled, becomes obsolete, or is voluntarily surrendered. Pilots may exercise these privileges at any airport. Pilots must also meet and maintain certain medical requirements and flight currency. Airman certificates conform to 49 U.S.C. 44703, applicable 14 CFR parts, as well as ICAO standards.

4.1 FAA Designees

Under 14 CFR Part 61, a pilot may apply for a certificate, rating, or authorization by making application to an authorized FAA designated examiner or through an FAA inspector at a FSDO. FAA inspectors are responsible for inspection, surveillance, enforcement, and investigation, and perform a limited number of airman certification activities. The FAA utilizes approximately 2,900 authorized designated pilot examiners to conduct the majority of certifications for pilots. Operating under FAA guidance and oversight, designees perform approximately 96 percent of all FAA pilot certification activity. Designees minimize the burden on pilot certification. Therefore, designees are an integral part of the FAA's current certification infrastructure and the pilot community relies on designees to perform their certifications. The crucial work of FAA inspectors, who would bear the burden of additional certification duties, could suffer if designees were not used for the issuance of improved pilot certificates.

4.2 Pilot Certificates

As of April 1, 2013, there were approximately 837,000 active pilots certificated by the FAA. The FAA issues Student, Sport, Recreational, Private, Commercial, and Airline Transport Pilot certificates as well as other airmen certificates. Between 2008 and 2012, the FAA's Flight Standards Service issued an average of 186,000 pilot certificates a year, including: Student pilot (3,600), Sport (1,500), Recreational (85), Private (77,500), Commercial (49,000), and Airline Transport Pilot (54,000). Except for those issued to student pilots, these certificates are made of high-quality plastic card stock and contain such tamper- and counterfeit-resistant features such as micro printing, a hologram, and a UV-sensitive layer, which complies with the American National Standards Institute and applicable FIPS 201-1 subsections. Additionally, the FAA's Office of Aerospace Medicine, which also has the authority to issue a combined student pilot certificate and medical certificate, issued an average of 37,000 student pilot certificates per year between 2007 and 2011.

The paper student pilot certificate contains the same information as a plastic certificate, but also provides an area for a Certified Flight Instructor to endorse. The endorsement represents a specific aircraft (make and model) that the student has been trained to operate. The student certificate also contains a solo endorsement area, which allows the student pilot to operate a specific aircraft as the sole occupant. A student pilot certificate is issued with an expiration date of up to 60 months from the month of issuance, depending on the age of the pilot. The Civil Aviation Registry maintains a database of all issued student pilot certificates and this information is sent to TSA for vetting, as previously described. As discussed later within the report, rulemaking is required to upgrade paper student pilot certificates, as well as temporary airman certificates, to improved pilot certificates.

Historically, the pilot certificate's intended purpose is to show qualifications and limitations and has never been used as a security credential and is not used for physical access or utilized beyond the privileges shown on the pilot certificate for its intended

purpose. The FAA currently does not have the infrastructure in place to collect or to use biometrics.

4.3 Airports

The United States has 19,425 airports, seaports, and heliports currently in use. The majority of these airports are categorized as private and military facilities. The FAA does not directly oversee operations that are conducted at private or military airports. However, 14 CFR part 157 mandates that the FAA be notified if anyone establishes, alters, or permanently closes an airfield. This enables the FAA to maintain a central database of airport information for the general public. Beyond the self-reporting requirement, the FAA does not regulate the use of private and military airports. Individual state transportation authorities regulate privately used airports and the U.S. Department of Defense regulates military-use airports.

Public airports represent the remaining facilities that are categorized by the FAA. There are 5,171 airports classified as commercial service, reliever, and general aviation which are deemed to be for public use. Local or State governmental agencies, organizations, or individuals own or operate most of these facilities. The FAA prescribes minimum safety standards under 14 CFR part 139 if the airport hosts certain commercial operations, such as scheduled air carrier operations or unscheduled operations with large aircraft. As of June 17, 2013, there were 546 airports regulated under part 139 within the United States.

Many private, military, and public-use airports are eligible for FAA grants. Eligibility requirements for public airports are determined by the Airport Improvement Program (AIP). It cites the National Plan of Integrated Airport Systems report, which identifies 3,331 existing and proposed airports that are significant to air transportation. FAA Order 5100.38C, the Airport Improvement Program Handbook, provides guidance and sets forth policy to enable the distribution of funds from the FAA to individual public airports. The airports meet the basic eligibility requirements to receive funding from the FAA but are subject to limitations and stipulations for the use of the FAA funds.

TSA develops standards, policies, and guidance for airport security (including access controls) as set forth in 49 CFR part 1542. Under part 1542, approximately 450 individual airports are each responsible for complying with these security standards and paying for any necessary infrastructure. Access controls are technologies that prevent access by unauthorized persons into sensitive areas of an airport. These access control units are placed at secure entry points and employ various methods of determining an individual's rights to gain entry into a secure environment. The method for determining access is arbitrated by each individual airport, in accordance with TSA's standards, in part 1542.

Airports may receive AIP funding to install access controls; however, 49 U.S.C. § 47102 places limitations to AIP funding for any additional security improvements. The additional security improvements are eligible only at airports certificated by the FAA under 14 CFR part 139 and the AIP will fund a security project or specific piece of

security equipment only if it is required by regulation, which in this case is 49 CFR part 1542. These are identified in the TSA-approved airport security program as being a component or integral part of the overall security system. These improvements may include door controls, lighting of fencing/gates, keys and locks, closed circuit television monitors, and fingerprinting equipment needed for criminal history records checks of certain employees. Any security equipment beyond what is required by 49 CFR part 1542 is generally ineligible for AIP funding. Therefore, an individual airport would be responsible for funding such equipment.

5.0 Current Security Infrastructure Requirements

In accordance with 49 U.S.C. 44903, TSA has statutory authority to prescribe regulations requiring airports to establish security programs that protect the safety of air passengers, approve such security programs, and develop sanctions for use as guidelines in the discipline of employees for infractions of airport access control requirements. Each airport is responsible for developing and implementing a security plan that best fits its unique physical and operational characteristics and security requirements. Additionally, each airport, like other transportation facility owner/operators, holds the final decision as to who may access its sterile and secured areas.

TSA reviews and approves airport security programs to ensure they meet the requirements of 49 CFR part 1542. However, TSA does not have funding or provide funding to implement security measures or access control systems. Airport infrastructure improvements are funded through a combination of revenue generated from an airport's operations, funding from State and local governments, and FAA grants. TSA does not dictate the specific technology an airport operator must use; rather, it requires that the access control measures meet specific performance standards. Additionally, TSA, in accordance with 49 U.S.C. 44903, worked with the aviation and biometrics industries and the National Institute of Standards and Technology (NIST) to establish guidance on the use of biometrics in an airport access control system. Airports have access to and use that guidance in the development of access controls that reflect each airport's characteristics and security needs.

6.0 Certificate Standards

Section 321 requires the FAA to issue improved pilot certificates as smart cards that are compliant with Federal Information Processing Standards 201 (FIPS 201) or Personal Identity Verification – Interoperability Standards (PIV-I) for processing through security checkpoints into airport sterile areas.

6.1 FIPS 201-1

FIPS 201-1 is a standard for verifying personal identity for Federal employees and contractors in order for a Federal entity to issue an identity card. FIPS 201-1 was established by NIST in March 2006 and titled Personal Identity Verification (PIV) of Federal Employees and Contractors. NIST established the standard to meet the requirements of the Homeland Security Presidential Directive 12 (HSPD12), which was issued by President Bush on August 27, 2004.

The standard established by FIPS 201-1 is based on secure and reliable forms of identification credentials issued by the Federal Government. The standard is organized into two parts. The first part describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD12. The second part provides detailed technical specifications to support the control and security objectives in part one as well as interoperability among Federal departments and agencies. All sections in the FIPS 201-1 are mandatory for Federal agencies and their contractors unless it is otherwise stated.

Although FIPS 201-1 does not describe the policies and minimum requirements for a PIV-I card, the Federal Chief Information Officers (CIO) Council has adopted guidance to non-federal issuers that allows interoperability of credentials. The physical characteristics, storage media and data elements specified in FIPS 201-1 also have been adopted by the Federal CIO PIV-I document. The standard also sets forth the required biometric information contained on a smart card. FIPS 201-1 allows for fingerprints and a photograph but it currently does not permit any other biometric information. The requirements for collecting and formatting biometric information are specified in NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification. New biometric data must be collected every 5 years for card reissuance. The card must also be revalidated every 3 years.

NIST has published a draft FIPS 201-2 that will enable the use of iris biometric data, among other changes. NIST is reviewing public comments to FIPS 201-2 and has not yet established this standard.

FIPS 201-1 supports a fingerprint biometric identifier required by Section 321(c)(3)(A) but does not accommodate the use of iris biometric data. Instead, a facial image is used, meaning an authorized individual performs a visual comparison of the photograph to the individual presenting the identification. This would provide greater security than an iris

biometric particularly if the person making the comparison of the card to the individual does not have a card reader

6.2 PIV-I

The PIV-I card is an identity card that meets the FIPS 201-1 standard. A PIV-I card is issued to an individual not associated with the Federal government; however, the Federal government is allowed to trust the card. Nevertheless, the PIV-I cards do not guarantee access of any kind to a federal or private facility. The individual facility has the authority to recognize a PIV-I card, and such recognition is not mandatory for any entity. However, if a Federal, State, or private entity chooses to accept a PIV-I card as identification and gaining physical access to a facility, the card is able to work with the infrastructure for Federal relying parties to trust the cards.

6.3 Potential Challenges to the Implementation Process

As discussed throughout this report, there are several challenges to adapting the FAA's pilot certification to Section 321 requirements and the FIPS 201-1 standard.

Any FAA rulemaking to implement the FIPS 201 standard for improved pilot certificates will have high costs to the FAA and public. The short validity period of the certificate, the durability of PIV-I cardstock, and the frequent reissuance and replacement of pilot certificates compounds this cost burden. Additionally, issuance of improved pilot certificates under FIPS 201-1 require face-to-face visits to enrollment centers, which creates high travel costs for certificate applicants (especially those in rural areas where enrollment centers are more dispersed). Moreover, because the access functionality of the improved pilot certificate is controlled locally at each individual airport, many pilots may realize few access benefits after incurring the costs for the certificate.

The FAA and TSA have been working closely to identify various approaches to overcome these challenges. This process will continue throughout the FAA rulemaking project and through the interagency working group. For example, the FAA is considering issuance of an improved pilot certificate that is aligned with FIPS 201-1. This alignment would take advantage of the most effective elements of the standard while also reducing costs of implementing all elements.

7.0 Rulemaking Required

To implement the requirements of Section 321, the FAA must conduct rulemaking. The FAA has initiated a rulemaking project to issue pilot certificates that would be a smart card that can accommodate a photograph and biometric data. 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. The FAA is considering several options for the issuance of the improved pilot certificates to mitigate costs associated with those requirements. The FAA is also evaluating how to reconcile the statutory mandate (requiring fingerprint and iris biometric) and the FIPS 201-1 standard (supporting only a fingerprint biometric). Accordingly, it is difficult to project a timeline for the issuance of improved pilot certificates.

7.1 Potential Costs to the Public and the FAA for Issuing Improved Pilot Certificates

The FAA does not have access to a cost estimate for infrastructure necessary to take advantage of information contained on improved pilot certificates.

Any rulemaking requiring photographs and biometric data on pilot certificates would impose costs on pilots and the FAA. The TSA has experience issuing cards similar to those required by Section 321. The FAA used TSA's experience to calculate the costs based on a reasonable program consistent with Section 321 and the FIPS 201-1 standard. The FAA assumes that biometric collection and certificate activation would occur at an existing TSA enrollment center or other FAA-approved location. The FAA analyzed the costs associated with initial issuance, renewal, and replacement of improved pilot certificates based on experience from existing airman certification. However, it must be emphasized that the actual amount of these potential costs associated with any program for issuing such pilot certificates would be determined only through FAA rulemaking.

Based on preliminary analysis, the total costs to all parties involved in this process over 12 years (initial implementation period and 2 renewal cycles) is estimated at approximately $1.125 billion. This includes the travel cost to applicants for application and certificate activation. It also includes the FAA processing costs for issuing a pilot certificate. The FAA must charge cost recovery fees pursuant to Section 122 of Public Law 112-95, which means the applicant would pay most FAA processing costs as a certificate fee. Therefore, the actual out-of-pocket pilot costs would be a significant portion of that total cost. Additionally, to the extent that TSA enrollment centers or FAA designees are used, the pilot likely would pay their processing costs, which are not included in this estimate. As noted above, this estimate does not include costs for infrastructure to take advantage of information contained on improved pilot certificates.

Through the rulemaking process, the FAA is evaluating a variety of alternatives to reduce this overall cost as well as the out-of-pocket costs to certificate holders and applicants.

The FAA expects to present an analysis of these alternatives in the notice of proposed rulemaking.

8.0 Recommendations for Federal Installation of Infrastructure

The FAA recognizes that TSA is the Federal agency that governs airport security, and TSA has supported the issuance of biometric access control guidelines for airports to use. Any additional access control requirements relating to security should continue to be governed by TSA. The FAA recommends that individual airports continue to identify the infrastructure necessary to ensure proper access control and to take advantage of information contained on improved pilot certificates that the FAA intends to issue. The FAA will continue to work with TSA concerning the issuance of improved pilot certificates. To the extent possible, the FAA will issue certificates that are compatible with the TSA's approved security infrastructure and overall security requirements.

Appendix 1: Excerpt from the Federal Aviation Administration Modernization and Reform Act of 2012 (Public Law 112-95)

SECTION 321. IMPROVED PILOT LICENSES

(a) IN GENERAL.—The Administrator of the Federal Aviation Administration shall issue improved pilot licenses consistent with requirements under this section.

(b) TIMING.—Not later than 270 days after the date of enactment of this Act, the Administrator shall—
(1) provide to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report containing—
(A) a timeline for the phased issuance of improved pilot licenses under this section that ensures all pilots are issued such licenses not later than 2 years after the initial issuance of such licenses under paragraph (2); and
(B) recommendations for the Federal installation of infrastructure necessary to take advantage of information contained on improved pilot licenses issued under this section, which identify the necessary infrastructure, indicate the Federal entity that should be responsible for installing, funding, and operating the infrastructure at airport sterile areas, and provide an estimate of the costs of the infrastructure; and
(2) begin to issue improved pilot licenses consistent with the requirements of title 49, United States Code, and title 14, Code of Federal Regulations.

(c) REQUIREMENTS.—Improved pilot licenses issued under this section shall—
(1) be resistant to tampering, alteration, and counterfeiting;
(2) include a photograph of the individual to whom the license is issued for identification purposes; and
(3) be smart cards that—
(A) accommodate iris and fingerprint biometric identifiers; and
(B) are compliant with Federal Information Processing Standards-201 (FIPS–201) or Personal Identity Verification-Interoperability Standards (PIV–I) for processing through security checkpoints into airport sterile areas.

(d) TAMPERING.—To the extent practicable, the Administrator shall develop methods to determine or reveal whether any component

or security feature of an improved pilot license issued under this section has been tampered with, altered, or counterfeited.

(e) USE OF DESIGNEES.—The Administrator may use designees to carry out subsection (a) to the extent practicable in order to minimize the burdens on pilots.

(f) REPORT TO CONGRESS.—
(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Administrator shall submit to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the issuance of improved pilot licenses under this section.
(2) EXPIRATION.—The Administrator shall not be required to submit annual reports under this subsection after the date on which the Administrator has issued improved pilot licenses under this section to all pilots.