AAL AK E5 Deering, AK [New]

Deering Airport, AK

(Lat. 66°04′10″ N., long. 162°45′59″ W.)

That airspace extending upward from 700 feet above the surface within a 7-mile radius of the Deering Airport, and that airspace extending upward from 1,200 feet above the surface within a 45-mile radius of the Deering Airport, excluding the airspace outside 12 miles from the shoreline.

* * * * *

Issued in Anchorage, AK, on October 14, 2005.

Judith G. Heckl,

Area Director, Alaska Flight Service Operations.

[FR Doc. 05–21231 Filed 10–24–05; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF STATE

22 CFR Part 51

[Public Notice 5208]

RIN 1400–AB93

Electronic Passport

AGENCY: Department of State.

ACTION: Final rule.

SUMMARY: This rule amends the passport regulations to incorporate changes related to introduction of the electronic passport. The rule defines ''electronic passport,'' includes a damaged electronic chip as an additional basis for possible invalidation of a passport and provides for no fee issuance of a replacement passport if an electronic chip fails.

DATES: This rule is effective October 25, 2005.

FOR FURTHER INFORMATION CONTACT: Sharon Palmer-Royston, Office of Passport Policy, Planning and Advisory Services, Bureau of Consular Affairs on 202–663–2662.

SUPPLEMENTARY INFORMATION: This rule was originally published in the **Federal Register** on February 18, 2005 (70 FR 8305) as a proposed rule that included changes to the passport regulations needed due to the pending introduction of the electronic passport, as well as changes related to passport amendments, replacement passports, and unpaid fees that did not relate exclusively to electronic passports. Because of the volume of comments, we separated the proposed rule into two final rules. The first rule, RIN 1400-AC11, incorporated the provisions of the proposed rule on passport amendments, replacement passports, and unpaid fees. We received only two comments on those provisions. The second, and instant, rule focuses on electronic passports.

Analysis of Comments

We received a total of 2,335 comments on the introduction of the electronic passport. All comments have been read, sorted, and tabulated according to primary concerns. Comments opposing the proposed rule primarily focus on security and/or privacy, the adequacy of Radio Frequency Identification (RFID), technology, and religious concerns. Specifically, concerns focused as follows: 2019 comments listed security and/or privacy; 171 listed general objections to use of the data chip and/or the use of RFID; 85 listed general objections to use of the electronic passport; 52 listed general technology concerns; and 8 listed religious concerns. Overall, approximately 1% of the comments were positive, 98.5% were negative, and .5% were neither negative nor positive.

The comments are available for review at *http://www.travel.state.gov/,* under the passport section, or at the Department of State (Department) reading room.

Security and Privacy

Passports must be globally interoperable—that is, they must function the same way at every nation's border when they are presented. To that end, the International Civil Aviation Organization (ICAO) has developed international specifications for electronic passports that will ensure their security and global interoperability. These specifications prescribe use of contactless smartcard chips and the format for data carried on the chips. They also specify the use of a form of Public Key Infrastructure (PKI) that will permit digital signatures to protect the data from tampering. The United States (U.S.) will follow these international specifications to ensure its electronic passport is globally interoperable.

The Department intends to begin the electronic passport program in December 2005. The first stage will be a pilot program in which the electronic passports will be issued to U.S. Government employees who use Official or Diplomatic passports for government travel. This pilot program will permit a limited number of passports to be issued and field tested prior to the first issuance to the American traveling public, slated for early 2006. By October 2006, all U.S. passports, with the exception of a small number of emergency passports issued by U.S. embassies or consulates, will be electronic passports.

The ICAO specification for use of contactless chip technology requires a minimum capacity of 32 kilobytes (KB). The U.S. has decided to use a 64KB chip to permit adequate storage room in case additional data, or biometric indicators such as fingerprints or iris scans, are included in the future. Before modifying the definition of ''electronic passport'' to add a new or additional biometric identifier other than a digitized photograph, we will seek public comment through a new rule making process.

The contactless smart chip that is being used in the electronic passport is a ''passive chip'' that derives its power from the reader that communicates with it. It cannot broadcast personal information because it does not have its own source of power. Readers that are on the open market, designed to read Type A or Type B contactless chips complying with International Standards Organization (ISO) 14443 and ISO 7816 specifications, will be able to communicate with the chip. This is necessary to permit nations to procure readers from a variety of vendors, facilitate global interoperability and ensure that the electronic passports are readable at all ports of entry.

The proximity chip technology utilized in the electronic passport is designed to be read with chip readers at ports of entry only when the document is placed within inches of such readers. It uses RFID technology. The ISO 14443 RFID specification permits chips to be read when the electronic passport is placed within approximately ten centimeters of the reader. The reader provides the power to the chip and then an electronic communication between the chip and reader occurs via a transmission of radio waves. The technology is not the same as the vicinity chip RFID technology used for inventory tracking of items from distances at retail stores and warehouses. It will not permit ''tracking'' of individuals. It will only permit governmental authorities to know that an individual has arrived at a port of entry—which governmental authorities already know from presentation of non-electronic passports—with greater assurance that the person who presents the passport is the legitimate holder of the passport.

The personal information that will be contained in the chip is the information on the data page of the passport—the name, nationality, sex, date of birth, place of birth, and digitized photograph of the passport holder. The chip will also contain information about the

passport itself—the passport number, issue date, expiration date, and type of passport. Finally, the chip will contain coding to prevent any digital data from being altered or removed as well as the chip's unique ID number. This coding will be in the form of a high strength digital signature. The contents of the data page of the traditional passport have been established by international usage and by ICAO. The chip will not contain home addresses, social security numbers, or other information that might facilitate identity theft.

In terms of the comments received in response to our proposed rule, a small minority of comments welcomed the rule because of the enhancements to passport security the electronic passport will provide, including better authentication of the document, proof of its link to the bearer and protection against data alteration than is provided by the current, traditional non-electronic passports. The vast majority of comments, however, opposed the introduction of the electronic passport on security and privacy grounds, specifically concerns that skimming or eavesdropping would permit surreptitious reading of the data contained in the passport chip. Skimming is the act of creating an unauthorized connection with a readable chip in order to gain access to the data contained therein. Eavesdropping is the interception of the electronic communication session between a passport chip and an authorized reader.

Comments reflected a concern that the data in the electronic chip could easily be read by portable devices available on the open market. Many of these comments expressed a belief that the information could be read at distances in excess of ten feet. The majority of the comments were concerned that terrorists could identify and target them as U.S. citizens. Identity theft was of grave concern, focusing on the potential for criminal activity resulting directly from identity theft. Some comments expressed fears that criminals could acquire and use the personal information included in the passport to target them for theft, con artist schemes and/or kidnapping. Still others expressed fears that the U.S. Government or other governments would use the chip to track and censor, intimidate or otherwise control or harm them. Some comments called for the inclusion of a fail-safe anti-skimming device.

The Department is sensitive to the security and privacy concerns raised by the comments. To address these concerns, the Department and the Government Printing Office (GPO) have worked with the National Institute of Standards and Technology (NIST) to evaluate the passport's vulnerability to skimming and to test physical devices that can be put in a passport to reduce its likelihood.

Based on that testing, the Department, in cooperation with the GPO, will include an anti-skimming material in the front cover and spine of the electronic passport that will mitigate the threat of skimming from distances beyond the ten centimeters prescribed by the ISO 14443 technology, as long as the passport book is closed or nearly closed.

The Department will also implement Basic Access Control (BAC) to mitigate further any potential threat of skimming or eavesdropping. BAC recently has been adopted as a best practice by the ICAO New Technologies Working Group and will soon be formally added to the ICAO specifications. BAC utilizes a form of Personal Identification Number (PIN) that must be physically read in order to unlock the data on the chip. In this case, the PIN will be derived from the printed characters from the second line of data on the Machine-Readable Zone that is visibly printed on the passport data page. The BAC also results in the communication between the chip and the reader being encrypted, providing further protection.

Shielding the reader or other measures associated with the chip reader can also minimize the possibility of eavesdropping. The Department of Homeland Security (DHS) is responsible for border inspections of travelers, and the provision and use of the equipment at U.S. ports of entry that will read the electronic passports. The DHS is working with NIST on reader security and communications issues.

We believe that the measures described in this rule adequately address the concerns raised by comments regarding security and privacy.

Objections to the Use of the RFID Technology

Some comments discussed a belief that the RFID technology is too faulty or otherwise inadequate to be used in passports. In particular, some comments asserted that the RFID technology could easily be hacked into or counterfeited, which would defeat its usefulness as a security measure. The Department is taking every measure to ensure that the RFID chips it uses are resistant to hacking and counterfeiting. The devices used in the U.S. electronic passport must be Evaluation Assurance Level 4+ certified or better. This third party certification is commonly used with other government smartcard initiatives and it provides assurance that the manufacturing process is auditable and secure.

Additionally, the government conducts regular security audits of its vendor partners and their processes to maintain the security of its travel documents. Finally, the contactless smartcard chip used in the electronic passport will be securely inserted into a highly tamper proof, newly redesigned travel document. The new passport document is itself highly tamper resistant.

According to certain comments, use of a contact chip would be preferable. However, contact chip technology was assessed and specifically excluded by the ICAO subcommittees during the development of their electronic passport specifications. Contact chip technology is primarily used in card formats, and does not easily adapt to fabrication in book-type formats. Contact technology requires the use of exposed contacts that need to make precise contact when inserted in a reader. Fabricating this technology in a book format in a way that facilitates reliable reading is problematic. Passports must be durable over their ten-year life. Passports using contact technology where a part of the passport book must be inserted into a reader would lead to enhanced wear and tear on the passport, thereby fostering unreliable passport book reading.

Other comments suggested that the passport data should be encrypted. The passport data on the chip does not require encryption in order to be secure and protected. It is the same data that is visually displayed on the passport data page. Instead of encrypting data, BAC will permit an encrypted communication session with the reader that will provide a similar protection while not requiring administrative key control issues.

Consequently, we have decided not to change the basic characteristics of the chip that we will use in the electronic passport or the data that it will contain. We will, as explained above, incorporate additional technology, including the anti-skimming material and BAC, to address concerns about skimming and eavesdropping. This will not require any change in the general definition of ''electronic passport'' contained in the proposed regulation. In this final rule, we have made a technical change to the language of the proposed definition to state that the chip will digitally carry information from the data page, a biometric version of the bearer's photo and coding protections.

Again, we believe that the measures described in this rule adequately address the concerns raised by comments regarding RFID technology.

Religious Objections

A small number of comments objected to the electronic passport due to religious beliefs. Without in any way passing judgment upon their beliefs, we do not consider these objections a basis for not proceeding with the proposed rule.

General Objections To Use of the Electronic Chip and Passport

Some comments stated that they objected to use of the electronic chip and passport, but did not give specific reasons for their objections. As a result, the Department is unable to formulate a useful response to their objections.

Regulatory Findings

Administrative Procedure Act

The Department is publishing this rule as a final rule, after publishing a proposed rule, allowing a 45-day provision for public comments, and consideration of all comments received. The Department provided for a shorter comment period than the 60 days suggested by Section 6(a) of E.O. 12866 because we believed 45 days would provide the public with a meaningful opportunity to comment while advancing important national security and foreign policy goals. We believe that the 2,335 comments received within that 45-day comment period validates this strategy. In order to protect the security of U.S. borders, it is essential that the Department implement the electronic passport program as soon as possible. In addition, a prompt launch of the program will increase our credibility and good will with other countries, which are implementing similar biometric passport programs.

Regulatory Flexibility Act/Executive Order 13272: Small Business

These changes to the regulations are hereby certified as not expected to have a significant impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act, 5 U.S.C. 601–612, and Executive Order 13272, section 3(b).

The Small Business Regulatory Enforcement Fairness Act of 1996

This rule is not a major rule, as defined by 5 U.S.C. 804, for purposes of congressional review of agency rulemaking under the Small Business Regulatory Enforcement Fairness Act of 1996, Public Law 104–121. This rule will not result in an annual effect on the economy of $100 million or more; a major increase in costs or prices; or adverse effects on competition, employment, investment, productivity, innovation, or the ability of United States-based companies to compete with foreign based companies in domestic and export markets.

The Unfunded Mandates Reform Act of 1995

Section 202 of the Unfunded Mandates Reform Act of 1995 (UFMA), Public Law 104–4, 109 Stat. 48, 2 U.S.C. 1532, generally requires agencies to prepare a statement before proposing any rule that may result in an annual expenditure of $ 100 million or more by State, local, or tribal governments, or by the private sector. This rule will not result in any such expenditure nor will it significantly or uniquely affect small governments.

Executive Orders 12372 and 13132: Federalism

This regulation will not have substantial direct effects on the States, on the relationship between the national government and the States, or the distribution of power and responsibilities among the various levels of government. Nor will the rule have federalism implications warranting the application of Executive Orders No. 12372 and No. 13132.

Executive Order 12866: Regulatory Review

The Department of State has reviewed this rule to ensure its consistency with the regulatory philosophy and principles set forth in Executive Order 12866 and has determined that the benefits of the regulation justify its costs. The Department does not consider the rule to be an economically significant regulatory action within the scope of section 3(f)(1) of the Executive Order since it is not likely to have an annual effect on the economy of $100 million or more or to adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities. However, the rule does have important policy implications and involves a critical component of upgrading border security for the United States. Accordingly, it has been provided to the Office of Management and Budget (OMB) for review.

Executive Order 12988: Civil Justice Reform

The Department has reviewed the regulations in light of sections 3(a) and 3(b)(2) of Executive Order No. 12988 to eliminate ambiguity, minimize litigation, establish clear legal standards, and reduce burden.

The Paperwork Reduction Act of 1995

The portion of the proposed rule contained in this final rule does not impose any new requirements for the collection of information under the PRA.

List of Subjects in 22 CFR Part 51

Passports and visas.

■ Accordingly, the Department amends Part 51 of 22 CFR as follows:

PART 51—[AMENDED]

■ 1. The authority citation for part 51 continues to read as follows:

Authority: 22 U.S.C. 211a, 213, 2651a, 2671(d)(3), 2714 and 3926; 31 U.S.C. 9701; E.O. 11295, 3 CFR, 1966–1970 Comp., p 570; sec. 236, Public Law 106–113, 113 Stat. 1501A–430; 18 U.S.C. 1621(a)(2).

■ 2. Amend § 51.1 to add a new paragraph (j) to read as follows:

§ 51.1 Definitions.

* * * * *

(j) *Electronic passport* means a passport containing an electronically readable device, an electronic chip, encoded with the information printed on the data page, a biometric version of the bearer's photograph, a unique chip number, and a digital signature to protect the integrity of the stored information.

■ 3. Revise § 51.6 to read as follows:

§ 51.6 Damaged, mutilated or altered passport.

Any passport which has been materially changed in physical appearance or composition, or contains a damaged, defective or otherwise nonfunctioning electronic chip, or which includes unauthorized changes, obliterations, entries or photographs, or has observable wear and tear that renders it unfit for further use as a travel document may be invalidated.

■ 4. Amend § 51.64 to add a new paragraph (e) to read as follows:

§ 51.64 Replacement passports.

* * * * *

(e) When a passport is issued for the balance of the original validity period to replace a passport with a failed electronic chip.

Dated: October 19, 2005.

Maura Harty,

Assistant Secretary for Consular Affairs, Department of State.

[FR Doc. 05–21284 Filed 10–24–05; 8:45 am]

BILLING CODE 4710–05–P