

Interpreter Releases
Report and analysis of immigration and nationality law

© 2006 Thomson/West.

October 2, 2006

*2093 6. E-Passport Readers Installed at San Francisco Airport

On September 27, 2006, the U.S. Department of Homeland Security (DHS) completed deployment of e-passport readers at San Francisco International Airport in California. Installation of the new readers is the first in a series of planned deployments that DHS states will continue at U.S. airports through the next few weeks to meet the October 26, 2006, congressional deadline requiring U.S. ports of entry to compare and authenticate data in electronic passports (e-passports) issued by Visa Waiver Program (VWP) countries. [FN20]

Deployment of e-passport readers is the next step in a process that DHS hopes will further enhance the security of international travel documents while continuing to facilitate the flow of legitimate travel and trade to the U.S. An e-passport is designed to securely identify the individual holder, defend against identity theft, protect privacy, and make it difficult for individuals to cross borders using fraudulent documents. The e-passport carries the international e-passport symbol [FN21] on the cover and contains a contact-less chip with the passport holder's biographic information and a biometric identifier, such as a digital photograph of the holder. All e-passports issued by VWP countries and the U.S. have a critical security feature which prevents the unauthorized reading or "skimming" of data stored on the chip.

Editor's note: The safety of the chips, which incorporate radio frequency identification technology (RFID), [FN22] has been of public concern since the State Department began proposing electronic passport regulations. [FN23] Also, a number of publications have recently reported some major problems with the RFID chips. The Washington Post reports that the chips open up many possibilities for passport carriers to be subjected to unauthorized collection of data. [FN24] Wired Magazine on-line edition reports that not only can the RFID chips be cloned but also they can also be used to trigger explosive devices, which could *2094 make anyone carrying a U.S. e-passport the equivalent of an unsuspecting human detonator. [FN25]

The U.S. Border Security Act of 2002 [FN26] requires that passports issued by VWP countries on or after October 26, 2006, must be e-passports to be valid for entry into the U.S. without a visa and must comply with technical standards as established by International Civil Aviation Organization (ICAO). [FN27] As mentioned earlier in this article, the Act also requires that U.S. ports of entry have the capability to compare

and authenticate data from e-passports.

DHS states that, when applying to enter the U.S., travelers who have a valid machine-readable passport with a digital photograph do not need to obtain a new e-passport until the existing passport expires if the digital-photograph passport was issued before October 26, 2006. Also, the inspection process at a U.S. port of entry does not change for an e-passport holder. U.S. Customs and Border Protection (CBP) officers will have the ability to read the e-passport's chip at inspection booths displaying the international e-passport symbol.

During the past two years, the U.S. government has been involved in efforts, largely through the ICAO, to work with VWP countries to test [FN28] and perfect technical standards making e-passports interoperable with readers at U.S. ports of entry.

The 27 countries currently participating in the VWP are: Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland and the United Kingdom. [FN29] DHS reports that approximately 13 million people each year travel to the U.S. under the VWP to study, conduct business, visit family, or tour the country.

Visitors who would like to verify whether or not their passport meet the requirements and deadlines for VWP travelers may wish to contact a U.S. consular office in their country.

[FN20]. For recent coverage of the approaching deadline, including reproduction of State Department guidelines for foreign travelers to the U.S., see 83 Interpreter Releases 1946, 1966 (Sept. 11, 2006).

[FN21]. The State Department has provided a Joint Photographic Experts Group (JPEG) file of the symbol on a Web page available on the Internet at http://travel.state.gov/images/e_ppt_logo.jpg. Also see State Department guidelines for foreign travelers to the U.S., reproduced as Appendix I in 83 Interpreter Releases 1946, 1966 (Sept. 11, 2006).

[FN22]. RFID is a wireless technology that stores and retrieves data remotely from devices. Systems employing RFID technology include tags and readers on the front end and applications and databases on the back end. The technology allows sensitive information to be read and written to tags and for numerous tags to be scanned simultaneously from a distance. See 82 Interpreter Releases 1317 (Aug. 15, 2005) discussing implementation of RFID testing at certain land border crossings.

[FN23]. See 82 Interpreter Releases 1759 (Oct. 31, 2005).

[FN24]. See "The ID Chip You Don't Want in Your Passport," *The Washington Post*, A21 (Sept. 16, 2006), available through Westlaw® (2006 WLNR 16254199).

[FN25]. See "Hackers Clone E-Passports," *Wired* (Aug. 3, 2006), available through the Internet at <http://www.wired.com/news/technology/0,71521-0.html>.

[FN26]. Pub. L. No. 107-173, 116 Stat. 543. See 79 Interpreter Releases 769 (May 20, 2002).

[FN27]. The ICAO is the specialized agency within the United Nations that ensures the "safe, efficient, and orderly evolution of international civil aviation." The ICAO specifications prescribe the use of contact-less smartcard chips and the format for data carried on the chips. They also specify the use of a form of public key infrastructure

that will permit digital signatures to protect the data from tampering. For further information regarding the ICAO and the technical standards for e-passports, see the ICAO report on machine-readable travel documents (MRTDs) available on the Internet at http://www.icao.int/mrtd/download/documents/MRTD_Rpt_V1N1_2006.pdf.

[FN28]. DHS began conducting live testing of e-passports and e-passport readers on January 15, 2006, at the San Francisco International Airport. See 83 Interpreter Releases 167 (Jan. 23, 2006).

[FN29]. Editor's note: Belgium was the first country to have completed its rollout of e-passports. See 82 Interpreter Releases 745 (May 2, 2005). Only about half of these countries were certified as having complied with the e-passport requirements as of September 6, 2006. See 83 Interpreter Releases 1946 (Sept. 11, 2006).

END OF DOCUMENT