# US passports to contain remotely readable computer chips

**Mike Ingram**
**29 October 2005**

The State Department issued a final rule October 25 for the implementation of new electronic passports. The so-called e-passport will come into effect October 2006, requiring all new US passports to include a radio frequency ID (RFID) chip that can transmit personal information, including the name, nationality, sex, date of birth, place of birth and a digitized photograph of the passport holder. The chip will be 64KB in size to leave room for additional biometrics data to be added in the future.

The decision was taken despite significant and continuing opposition from civil liberties groups and technical experts. Its implementation represents the latest step in a series of measures implemented in the wake of the 9/11 terror attacks attacking basic civil liberties of the US population.

The rule was originally published on February 18, 2005 and received a total of 2,335 comments, 98.5 percent of which were negative and only 1 percent positive. The Federal Register of October 25 states, "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 technology concerns; and 8 listed religious concerns." Yet the State Department final ruling in no way addresses the most significant of these concerns.

A comment prepared jointly by the Electronic Frontier Foundation (EFF) and a number of other privacy organizations and individuals states, "the proposed RFID passport will indiscriminately expose Americans' personal information to others." The document, submitted April 4, 2005, adds, "because this exposure can occur whenever and wherever a person carries the RFID passport, unauthorized persons—from government or private sector—could link passport holders to their activities in particular places."

The comment states further, "One's name may be public; one's face may be public; but it is an entirely different matter from a privacy perspective if a passport holder's identity can be ascertained by anyone with the right equipment when he or she is at a doctor's office, place of worship, or antiwar demonstration."

Opponents have focused on the decision to use the contactless technology of RFID, rather than a device such as the magnetic strips found in credit cards, door swipes and other devices. While the State Department claims that such technologies do not lend themselves to being placed inside a booklet-type passport, experts insist that there are no valid technical reasons for such a decision. There is concern that the decision to use RFID is precisely because the chip can be read remotely. This means that information can be gathered without the passport owners' knowledge or consent.

The ruling dismisses such concerns, stating, "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," adding that the RDIF specification used "permits chips to be read when the electronic passport is placed within approximately ten centimeters of the reader."

The rule states: "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."

While it is true that the specification ISO 14443 used in government scanners states a proximity of ten centimeters, the chips will be accessible by other readers that do not conform to this specification. Security expert Bruce Schneier points out in his

weblog, “Unfortunately, RFID chips can be read by any reader, not just the ones at passport control. The upshot of this is that travelers carrying around RFID passports are broadcasting their identity.

“Think about what that means for a minute. It means that passport holders are continuously broadcasting their name, nationality, age, address and whatever else is on the RFID chip. It means that anyone with a reader can learn that information, without the passport holder’s knowledge or consent. It means that pickpockets, kidnappers and terrorists can easily—and surreptitiously—pick Americans or nationals of other participating countries out of a crowd.

“It is a clear threat to both privacy and personal safety, and quite simply, that is why it is bad idea. Proponents of the system claim that the chips can be read only from within a distance of a few centimeters, so there is no potential for abuse. This is a spectacularly naïve claim. All wireless protocols can work at much longer ranges than specified. In tests, RFID chips have been read by receivers 20 meters away. Improvements in technology are inevitable.”

The Bush administration has provided no evidence that the chip will not permit tracking, but simply expects to be taken at its word—this from a government which has launched an illegal war in Iraq and countless attacks on democratic rights at home on the basis of proven lies.

As the EFF document points out, the rule contains “no discussion whatsoever of the alleged problem to be solved by the use of RFID technology in the US passport. Instead, it assumes the existence of problems such as lack of security, without ever demonstrating that these problems actually exist. If there is any factual record evidence that current US passports are insecure, it is neither presented nor cited here. It must be remembered that identity verification—knowing who someone is—does not by itself provide security. Many of the 9/11 hijackers used their true names and presented authentic identification credentials.”

No such evidence was presented in the final ruling because the reality is that the introduction of electronic passports, like other measures taken by the Bush administration in the aftermath of the terrorist attacks of 2001, has nothing to do with protecting people against terrorism. Rather, it is a further confirmation that the “war on terror” is being used as a pretext to destroy democratic rights at home.