

# DHS Privacy Committee Finalizes Report on RFID IDs

DHS Secretary Michael Chertoff will soon receive the 15-page advisory report, which the coauthors hope will impact the U.S. government's approach to incorporating RFID technology in identification documents.

By Mary Catherine O'Connor

Dec. 12, 2006—A revised version of a report from the [Data Privacy and Integrity Advisory Committee](#), a subcommittee of the [Privacy Office of the U.S. Department of Homeland Security](#) (DHS), was cleared for publication at a Dec. 6 meeting of the committee in Miami Beach, Fla. The report, titled "[The Use of RFID for Human Identification](#)," will now be sent to DHS Secretary Michael Chertoff, as well as the DHS's chief privacy officer, Maureen Cooney.

The subcommittee wrote the 15-page report to guide Chertoff and Cooney in deciding whether to deploy RFID technology to identify or track individuals for such DHS programs as the PASS cards that will eventually be issued as an alternative to U.S. passports for travel in North America.

The [original version of the report](#), written by the committee's Emerging Applications and Technology Subcommittee, was presented to the full Advisory Committee on June 7, 2006, at a public meeting in San Francisco (see [DHS Meeting Draws Comments on RFID](#)). At the time, it received a chilly reception by many representatives from companies selling RFID technology used in identification and credential applications, as well as from technology industry groups, because it came down hard on the use of RFID in identity documents. "We recommend that RFID be disfavored for identifying and tracking human beings," the draft report indicated, citing concerns over the skimming of personal data transmitted over a radio frequency signal, the cost of implementing RF technology and the existence of other authenticating technologies that could be used instead.

The final version of the report comes to a similar conclusion, according to coauthor Jim Harper, a director of information-policy studies for the [Cato Institute](#), though its language has been softened. "I think a lot of the language was toned down, and a lot of assumptions that I feel strongly are true...were left out for the sake of congeniality," he says. One example he points to is the removal of most descriptions of RFID in identity documents as being "a tracking technology." Still, he says, there are no "recognizable substantive changes" to the latest version.

But in his reading of the latest report, Douglas Farry, a managing director and chair of the RFID practice at [McKenna Long & Aldridge](#), a nationwide law firm focusing on the intersection of public policy and technology, sees a more pronounced change in the final draft. "It seems to be a better position than the initial draft, in that the initial draft concluded that the potential benefits [of using RFID in identity documents] were more than outweighed by the potential risks to personal privacy [that the technology presents]. But that's toned down. Now it says that if the DHS is going to use an RFID system, it should do so thoughtfully and carefully."

Both the original and revised reports are roughly the same length, and both share a common architecture and most of the same section and subsection content. However, the original version uses more pointed language. For instance, both versions state that RFID can provide a means of identifying a credential, but not the individual who is presenting it. To authenticate the bearer, they say, one or more biometric scans must be used to prove the credential was issued to the person presenting it. The two versions of the report diverge, however, in regard to the impact that authenticating the bearer would have on the process of RFID use to authenticate the document. "The steps needed to verify the biometric information using today's technology may reduce or negate the speed benefit offered by radio transmission," the revised report states. The original, however, contains the following wording: "Tying RFID to a biometric authentication negates the speed benefit [of using RFID]."

The reports also differ in describing the possible risks to personal privacy presented by the use of RFID technology in identity documents. The original version of the report says, "The use of RFID for human identification may create a number of risks that are not found in conventional and non-radio identification processes. Individuals will likely be subject to greater surveillance in RFID identification. They will be less aware of being identified and what information is transferred during identification, concerns that necessitate transparency in the design of RFID identification systems." In contrast, the revised report focuses on the personal-privacy risks created by any digital information system, over a manual system. "Digital identification systems pose privacy risks," the revised report states. "In a visual ID-check environment, a person may be briefly identified but then forgotten, rendering them anonymous for practical purposes. In a digital (RF-based) identity-check environment, by contrast, a person's entry into a particular area can be recorded and the information stored for some period of time. If not properly protected, this information could also be repeatedly shared or used for secondary purposes, even potentially used for broader surveillance."

Harper says he hopes members of the DHS and representatives from the RFID and smart-card industry will take the report to heart, giving credence to the best practices and privacy-focused safeguards it recommends.

The DHS and the U.S. Department of State (DOS) are already beginning to embed RFID inlays in U.S. passports, so the final publication of the privacy report comes too late for use by those agencies in that regard. Still, Harper maintains, the report could still hold value to decision makers in other countries who are considering deploying electronic passports. The guidelines the United States and other nations are following for deploying RFID in passports, Harper says, were devised by the International Civil Aviation Organization (ICAO), do not require as many privacy safeguards as they should (see United States Sets Date for E-Passports).

The DHS and DOS also plan to RFID-enable the PASS card, a travel document that will be issued in lieu of a U.S. passport to identify U.S. citizens who travel to Mexico, Canada, the Caribbean or Bermuda (see New U.S. ID for Border Crossing to Use RFID). The agencies originally set a deadline of Dec. 18 for the public to submit comments on their plans to add RFID to the card (see DHS Proposes Vicinity RFID Technology for PASSport Card). That deadline has now been extended to Jan. 8, and Harper says the Data Privacy and Integrity Advisory Committee hopes the agencies consider the report along with the public comments they are currently receiving, as they develop the PASS program.

RELATED\_ARTICLES For both electronic passports and the PASS card, the government wants to use RFID technology to increase document security and streamline documentation-verification procedures at checkpoints. While high-frequency (HF) inlays have a read range of just a few centimeters and are being deployed in passports with data-encryption capabilities, the agencies' plans for the PASS card call for the use of ultrahigh-frequency (UHF) inlays, which have a much longer read range and have not been made available with data-encryption capabilities. As a result, the Smart Card Alliance—an industry group made up of companies that manufacture HF-based ID and payment cards—is protesting the current PASS plans and

calling for the DHS and DOS to use HF inlays compliant with the ISO 14443 standard instead. The latter, the Alliance says, include data-encryption tools, whereas UHF tags do not.

Randy Vanderhoof, executive director of the Smart Card Alliance, says UHF has not been utilized within identity documents. Although the State Department seeks creative solutions to security from UHF technology vendors in its PASS-card proposal document, Vanderhoof adds, there are no such solutions on the market today. "We are concerned that the PASS card is being designed without good review of the privacy protections that are required," he says, "and that this won't happen until it's too late. That would be a mistake."

Copyright ©2005 RFID Journal, Inc. All Rights Reserved