

# DHS Meeting Draws Comments on RFID

RFID and auto-ID industry representatives, as well as privacy advocates and concerned citizens, gathered to discuss Homeland Security's "Use of RFID in Human Identification" report.

By Mary Catherine O'Connor

June 9, 2006—An eclectic mix of RFID industry representatives, general auto-ID industry members and concerned citizens gathered at the Clift Hotel in San Francisco on Wednesday for a meeting of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Attendees provided and heard commentary on a draft report released last month, written by the committee's Emerging Applications and Technology Subcommittee, entitled "The Use of RFID in Human Identification."

The Data Privacy and Integrity Advisory Committee makes recommendations to Michael Chertoff, secretary of homeland security, and Maureen Cooney, the department's acting chief privacy officer. The committee focuses on programmatic, policy, operational, administrative and technological issues relevant to the DHS that affect individual privacy, data integrity and data interoperability. The draft report is intended to guide the department on its use of RFID technology in identity documents. Citing concerns over misuse and possible shortfalls of the technology with respect to privacy protections, the report suggests the DHS consider alternatives to using RFID in identity documents (see DHS Subcommittee Advises Against RFID).

The written comments, submitted to the committee before May 22, were shared with the meeting attendees. The majority were from citizens and privacy advocates, expressing concern—or, in many cases, outrage—over the use of RFID technology in government identity documents (or other applications of the technology, including using tags to identify pharmaceuticals), and citing fears that the government would use the tags for surveilling citizens.

A number of individuals, however—mostly those representing companies in RFID or auto-ID industry associations—disagreed with the subcommittee's findings, stating they believe data encryption and other security measures make RFID appropriate for use in RFID. Written comments listed a number of concerns over how the draft report discusses possible misuses of RFID without also supplying details of such misuse. For example, a letter sent by Symbol notes that while the report states that "an eavesdropper may be able to collect usable information from communication between an RFID chip and reader, even if the communication is encrypted," it does not offer any "examples of how well-encrypted transmissions would offer useful information to an eavesdropper."

Steve Yonkers, privacy officer for the US-Visit Program, discussed how US-Visit is currently performing a proof-of-concept test to see how well UHF tags can be read from a distance when embedded in I-94 visa forms carried by foreign nationals as they enter and exit the country at land borders. Yonkers says US-Visit is testing the technology because it could help speed up the authentication process by prompting the computer screen used by U.S. Customs and Border Protections agents with the biometric data they need to check I-94 form-holders wishing to cross the border. The technology would also run the IDs against background checks to screen for possible criminals or terror suspects, prior to their arrival at the border checkpoint.

A representative of the [Smart Card Alliance](#), a not-for-profit association made of members of the contact-based smart card and RFID (or contactless) smart card industries, told the committee that US-Visit's use of UHF RFID is "not a secure approach." He added that only certain types of HF tags and readers—which the Smart Card Alliance calls contactless smart card technology, rather than RFID technology—are appropriate for identity documents, because they offer proven and standards-based data protection protocols. UHF technology, he says, is "subject to attacks."

Dan Mullen, president of [AIM Global](#), said the subcommittee's report was based on "misunderstandings" about what RFID technology is and what it can or should be used for. He said these misunderstandings are "generated by addressing RFID as a monolithic technology" rather than as a range of technologies with differing read ranges and security safeguards.

Industry representatives suggested that rather than basing its recommendations around specific technology, the committee should instead establish privacy and security policies independent of technology. Then, once that framework is set, they recommended applying standards-based technology compliant with that policy.

During the afternoon, panels discussed the expectations of privacy in public places and identity authentication. Panel members delved into a high-level analysis of how citizens share information, and how that shared data may (or may not) be protected by the [Fourth Amendment to the U.S. Constitution](#). During the panels, [MIT](#) professor Daniel Greenwood invited committee members to consider MIT's briefings and white papers about RFID and identity management, available at [the MIT ECAP Web site](#).

The DHS's Clooney said the meeting presented a "great opportunity for people with divergent views to share them with the committee." She added that in developing its recommendations, the committee is starting from "a neutral position with respect to all technology" and appreciates the comments and education offered by members of the RFID industry.

Howard Beales, chair of the Data Privacy and Integrity Advisory Committee, said the subcommittee would now consider the comments and begin revising the draft document. Revisions will likely be discussed at the committee's next meeting in September, he added. Once the committee finalizes the report, it will be submitted, as an advisory, to Secretary Chertoff.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved