

US-VISIT RFID Trial Shows Security Holes

A report from the DHS Office of Inspector General highlights data security issues and recommends that US-VISIT develop and follow policy and procedures for its RFID system.

By Mary Catherine O'Connor

July 7, 2006—The US-VISIT program is failing to adequately protect personal data being stored in databases and collected via RFID inlays embedded in its I-94 visa forms, according to a report released last month by the Department of Homeland Security's Office of Inspector General. The report suggests the organization should design and follow policies and procedures regarding the use of RFID technology and protections around personal information linked to RFID tags.

In 2004, the DHS launched the US-VISIT program to heighten border security by taking digital fingerprints and photos of all non-U.S. visitors entering the country (see Homeland Security to Test RFID). The report is based on an audit the office performed to determine whether US-VISIT "has implemented effective controls to protect its mission-critical data processed by its RFID systems from unauthorized access."

The audit consisted of visits to the U.S. border point-of-entry stations, where the RFID-enabled forms are being tested, as well as interviews with US-VISIT and Customs and Border Patrol (CBP) personnel (US-VISIT is a CPB program). The audit examined the physical layer of the system—how the tags, readers and I-94 forms are used and secured—as well as whether adequate policies and procedures have been enacted to ensure the "confidentiality, integrity and availability" of data contained in the Automated Identification Management System (AIDMS). The latter is the system of record used by the US-VISIT program to maintain databases for storing information about foreign nationals entering and exiting the country. The audit was conducted between November 2005 and February 2006.

During the audit, a team from the Office of Inspector General used a tool called the Internet Security Systems' Database Scanner to review database settings and to detect and analyze vulnerabilities on database servers. It also used an RFID spectrum analyzer and an interrogator (reader) to attempt to read I-94 forms being carried by persons going through the ports of entry where the technology is being tested. While the DHS still considers the distribution and reading of RFID-enabled I-94 forms a proof-of-concept rather than a permanent technology deployment, it has distributed more than 150,000 of the forms.

The audit results of the AIDMS database reportedly "revealed some security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data [relating to person carrying I-94 forms]." The report says these vulnerabilities were based in the areas of user account and password management, and user-access permissions. The details of such vulnerabilities are removed from the redacted version of the report, [available online](#).

During the audit, the team was not allowed to use unauthorized interrogators to "communicate or read the Form I-94s at ports of entry." However, it was able to pull the record indicator (the unique ID encoded to each form's RFID inlay) from sample forms in a laboratory setting, using what the report deems a "more sophisticated reader," though the redacted report does not detail what type of interrogator was used in the lab.

Today, rather than any personally identifiable information, only a record indicator is encoded to the RFID inlays embedded in the forms. The report further recommends that US-VISIT strengthen the data security of its RFID layer if personal data is ever encoded to the form.

The audit team provided US-VISIT personnel with the technical reports detailing the database and technical vulnerabilities it found in the RFID program. It also recommended the US-VISIT program "develop and implement a policy that addresses security controls over all components of an RFID system and ensure that policies and procedures are being followed at all affected ports of entry."

In responding to the report and its recommendations, US-VISIT personnel say they concur with some of the findings and have already acted on strengthening security measures around account management in the AIDMS database. Regarding the establishment of RFID policy and procedures, however, James Williams, director of US-VISIT, disagrees. In a written response to the inspector general, Richard Skinner, Williams replies that while the program has already completed its own data security and privacy impact assessments, it lacks the authority to enact policy regarding RFID, and that such policy needs to be established by the DHS. The department has completed a draft Applications Implementation Guide for RFID, which US-VISIT staff is reviewing and will comment on to the DHS. Implementations of all procedures at ports of entry, Williams notes, is "under the purview of CBP."

Implementation of another DHS initiative that could include use of RFID technology will be delayed if any of a number of pending bills passes through Congress. Last week, the Senate Appropriations Committee approved an amendment calling for a delay to the Jan. 1, 2007, implementation deadline for the Western Hemisphere Travel Initiative, which mandates that anyone crossing a land border with the United States, including U.S. citizens, must present secure travel documents denoting citizenship and serving as proof of identity. Sponsors of the legislature feel the DHS is not yet prepared to implement the program properly.

In January, Homeland Security Secretary Michael Chertoff and Secretary of State Condoleeza Rice announced plans to introduce the PASS, an RFID-enabled ID card that U.S. citizens would use to comply with the Western Hemisphere Travel Initiative. The card is expected to be ready for use late this year.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved