



Testimony
for the
Radio-Frequency Identification
Documents (RFID) Hearing

before the

California Research Bureau

by

Carol Henton
Vice President, State & Local

31 October 2007

Information Technology Association of America
Western Region Office
San Mateo, CA
650-357-7728
chenton@itaa.org
www.itaa.org

Good morning. I, Carol Henton, Vice President for State & Local of the Information Technology Association of America (ITAA), a trade association representing over 300 of the nation's leading manufacturers and users of leading edge technology. I am responsible for our State & Local programs and our state public policy issues.

Due to the importance of the issues surrounding identification management, ITAA established a separate program offering for this issue over three years ago. We have in place a very active Identity Management Committee, which is comprised of over 70 companies that are responsible for producing the majority of government credentialing and identity management programs at the federal, state, and local levels. Our members include companies producing drivers licenses and other identity cards; managing federal, state and local smart card and identity credentialing programs; providing biometric devices, radio frequency identification technologies and middleware solutions; as well as performing background checks and other identity proofing and authentication services for government customers worldwide. I appreciate the opportunity to speak to you and the CRB's advisory board about the importance of RFID technology.

The use of RFID technology offers significant benefits in many areas, including supply-chain efficiency, ensuring accurate pharmaceutical drug tracking, safe handling of hazardous materials, food safety and in government and employer-issued identification. As RFID technology matures and applications proliferate, it has the potential to enable global commerce and spur American innovation and competitiveness, while providing significant improvements in safety and security. The range of usage of RFID technology is immense, and spans many different industries. RFID is often mentioned as one of a set of emerging and connective technologies that may potentially have an impact on business and daily life that is as profound as the rise of the Internet.

In order for RFID to continue to gain broad acceptance in the commercial marketplace, we recognize that public concerns about consumer privacy and data security must be addressed. The most frequently cited concerns relate to what information is collected about consumers and how that information is protected. It is important to note that a variety of existing laws on the federal and state level already exist, which protect against the misuse of personally identifiable information.

ITAA does not believe it is correct to assume that certain types of RFID technology should not be used in identification documents because they are inherently insecure. The security and privacy of an identification document does not hinge on one type of technology, but rather on a layered security approach. RFID can make documents more secure and help protect an individual's privacy. The incorporation of RFID technology into an ID card can protect against fraud and forgeries because it can require far greater sophistication in terms of security based on the technology and the application's requirements. This sophistication in turn will make forged documents more difficult to obtain from unauthorized issuers.

ITAA believes that with any kind of credentialing or identity management program, regardless of whether it is RFID enabled or not, the following guidelines should be used:

- All credentialing programs involving personally identifiable information (PII) should be built on strong privacy and security policies from conception.
- All programs must have strict information security practices and database protection measures in place to safeguard the information collected, stored and transmitted.
- The technology used should fit the business case and program objectives, therefore the State of California should be careful not to legislate technology winners or losers.
- The identity authentication, registration, and issuance processes should be separate, so the control of the process is not held by one entity.
- Whenever possible identity management solutions should be based on recognized industry standards.

A good identity management system will utilize multi-faceted identity verification and authentication techniques, secure credential production, and tamper-resistant documents with multiple security features. Only by making sure that the entire ID system, from beginning to end, is built up around the best technologies, business processes and people management practices can genuine security be achieved.

ITAA believes that it is important to let the application's needs both from a security, operational, and policy standpoint determine the best technical solution for the State of California. Technologies are continually being augmented and improved to match the user needs in all application areas; therefore, legislating a particular implementation ignores this basic fact and the need to encourage technological improvements to Radio Frequency Identification techniques -- as well as other emerging technologies. ITAA believes that it is up to the appropriate government agencies to define system performance requirements so that the appropriate technology is selected that best meets the performance requirements that have been defined.

We wish to caution the California Research Bureau against recommending to the legislature that they restrict the use of certain technologies for government issued identification documents. A blanket statement that RFID is inherently insecure and should not be used in credentials with personally identifiable information should not be made.

As an alternative to mandating legislative restrictions on RFID technology, ITAA believes policymakers should encourage government entities that are procuring identity systems to consider privacy and security requirements. ITAA believes that individual applications should define the level of security required, not legislative statute. The protection or level of security in RFID enabled identity documents needs to match the sensitivity of information that is contained on the document. A legislative mandated "one-size-fits all" approach is not appropriate.

Finally, we believe that RFID technology will continue to evolve and protections for this technology will also continue to evolve. For this reason, ITAA cautions against legislative efforts to lock in certain protections.

Thank you for this opportunity to provide comments as you conduct this important research effort.