

**Before the
DEPARTMENT OF HOMELAND SECURITY
Washington, D.C. 20528**

Regarding)
)
The DHS’s request for comments)
on the DHS Emerging Applications)
and Technology Subcommittee of the)
DHS Data Privacy and Integrity)
Committee’s draft report titled “The Use)
of RFID for Human Identification.”)

**COMMENTS OF AeA
(THE AMERICAN ELECTRONICS ASSOCIATION)
TO THE DEPARTMENT OF HOMELAND SECURITY
REGARDING
THE DRAFT REPORT,
“THE USE OF RFID FOR HUMAN IDENTIFICATION.”**

Executive Summary

AeA (the American Electronics Association) ¹ takes great exception over the approach the Draft Report takes in generalizing both the capabilities and uses of “RFID technology,” as there are many sweeping, unsubstantiated and incorrect generalizations made without pointing to scientific data, field tests or published reports. Specifically, the Draft Report:

- Disparages RF-enabled technologies through conclusory statements without the support of quantitative data;
- Uses generic definitions of “RFID,” which are detrimental to evaluating technologies and creating best practices;
- Misstates the fact that “tracking of human beings” is endemic to “RFID.” In fact, technology by itself is neutral – only those who control the data may track people; and
- Fails to note that certain RF-enabled technologies actually *enhance* the security and privacy of American’s personal information and data.

¹ AeA is the nation’s largest high-tech trade association, representing more than 2,700 companies with 1.8 million employees. These 2700+ companies span the high-technology spectrum, from software, semiconductors, medical devices and computers to Internet technology, advanced electronics and telecommunications systems and services. With 18 regional U.S. councils and offices in Brussels and Beijing, AeA has been the accepted voice of the U.S. technology community since 1943. For more information, please visit us at www.aeanet.org.

AeA does, on the other hand, applaud the Subcommittee on the Best Practices it recommends to the Secretary, and offers a rubric from which technology choices and implementations may be made. AeA recommends that:

- All technology choices should flow from a strong privacy and security policy;
- Strong privacy policies flow from accepted and even forward-looking practices; and
- Specific best practices be developed around RF-enabled technologies.

The overall thrust of AeA's comments can be summed up succinctly: *Don't ban technology, ban bad behavior*. It is AeA's respectful request that the Committee develop policies that protect personal privacy and security *first*, and *then* empower agency implementers to choose the technologies that will fulfill those policies. AeA further hopes that the Final Draft makes it clear that any conclusions about RF-enabled technologies be advisory for the Department of Homeland Security only, while the Best Practices and Security Policies stated should be considered, and implemented, throughout the Department.

AeA's Full Comments on the Draft Report

AeA (American Electronics Association) submits these comments in response to the Department of Homeland Security's ("DHS") request for comments regarding the DHS Emerging Applications and Technology Subcommittee ("the Subcommittee") of the DHS Data Privacy and Integrity Advisory Committee's ("the Committee") draft report entitled, *"The Use of RFID for Human Identification"* ("the Draft Report"). The protection of personal privacy is a highly regarded value which is shared by all Americans. Personal privacy can be preserved and even increased by the use of secure RF-enabled contactless integrated circuit chips in identity documents in combination with strong privacy policies and procedures. These comments will outline personal data privacy and RF-enabled technology best practices to be employed by government entities choosing the correct RFID technology for personal identification documents to be used by American citizens.

Our members realize the importance of protecting privacy and security, as these are the cornerstones of a free society. Because of Congress' efforts to protect Americans after the tragedy of September 11, 2001, and DHS's task to carry out Congress' mandates, we express support for DHS's leadership in approaching this critical issue, as well as the Committee and Subcommittee's efforts to balance the needs of safeguarding national security with that of ensuring American's privacy needs. However, AeA has strong concerns with the approach the Draft Report takes in generalizing both the capabilities and uses of "RFID technology," as there are many sweeping, unsubstantiated and incorrect generalizations made without pointing to scientific data, field tests or published reports. AeA does agree

with many of the existing and proposed best practices in managing identity documents, and would like to suggest additional best practices to further protect American's privacy and security.

The overall thrust of these comments can be summed up succinctly: *Don't ban technology, ban bad behavior*. It is AeA's respectful request that the Committee develop policies that protect personal privacy and security *first*, and *then* empower agency implementers to choose the technologies that will fulfill those policies. AeA further hopes that the Final Draft makes it clear that any conclusions about RF-enabled technologies be advisory for the Department of Homeland Security only, while the Best Practices and Security Policies stated should be considered, and implemented, throughout the Department.

Because the Draft Report disparages RFID technology without citing quantitative data, generalizes RFID technology and its applications, and arrives at conclusions not substantiated by fact, the Department may not arrive at the proper conclusions for protecting America's security.

The following comments will address major themes found in the Draft Report that we believe need to be addressed if the Committee is to properly determine the scope of use of technologies already found to be advantageous in protecting American's privacy and security. We hope that these observations will be helpful to the Subcommittee in preparing the next version of the Draft Report.

The Draft Report disparages RF-enabled technology without the support of quantitative data

First among AeA's concerns are the number of definitive qualitative statements and conclusions made regarding contactless identification technology. It is our fear that many of the conclusory statements made in the Draft Report regarding speed, security, and risks may be accepted as fact when they have been made without pointing to scientific data, field tests or published government reports. Specifically, generalizations towards read ranges and read rates are unsubstantiated by either anecdotal or actual data.

Also, a number of misstatements force readers into inappropriate conclusions. For instance, the examples of the I-94 Form and the ePassport would lead readers into the assumption that the I-94 Form is a poor implementation because it does not verify the identity of the holder. In the case of the ePassport implementation, the report concludes it is similarly poor because of the read speed. However, the Draft Report fails to note that the I-94 Form's final implementation was *never* designed to act as an identity document that authenticates its holder to the credential. Equally problematic is that the report does not mention the prime purpose of placing a contactless chip in the e-Passport was to specifically authenticate the holder to the credential, prevent tampering and forging, and facilitate confidence in verifying the data. Read rate speed of e-Passport was not a primary reason for the program but, read rate has been an

important criteria for the program. According to all accounts, the US Department of State, responsible for implementing the ePassport, is exceedingly satisfied with its continuing implementation.

AeA recommends that future versions of the Draft Report consider and cite the mission requirements and parameters of each program it references in order to give the Secretary an unabridged and clear view of the programs needs and the technology used relative to the government application.

Using a generic definition of “RFID” is detrimental to evaluating technologies and creating best practices.

Core to AeA member company concerns is the approach the Draft Report takes in addressing uses of RFID technology as the only means of identity management. Specifically, the Draft Report uses the term “RFID” in a generic manner, to denote any use of technology that utilizes the radio-frequency spectrum to facilitate remote identification for purposes of authorization, authentication and/or access. There are currently a number of different identification technologies that are available to authenticate people, many of which have standards certified by the International Organization for Standardization (ISO)², applications of which include proximity cards, proximity smart cards, and vicinity smart cards. ISO is currently finalizing another RF-enabled technology standard that may be beneficial for certain purposes within DHS, as well as a number of other RF-enabled technologies that have yet to apply for ISO certification.

While all of the RF-enabled technologies that can be implemented for identification purposes have their unique benefits and drawbacks with regard to specific mission criteria, the Draft Report does not differentiate between the varying RF-enabled technologies – from identity management, asset management or even animal identification. In fact, it seems as if the Draft Report confuses the attributes of *all* the varying technologies and applications into one overbroad generalization. While it is almost certain that this may have occurred due to the drafter’s desire for brevity, we believe that the conclusions the Draft Report convey will obfuscate the benefits, abilities and limitations of each of the RF-enabled technologies, to the detriment of:

1. The Secretary’s ability to differentiate which technology is best applied to a particular application and the best practices and policies determined by DHS;
2. The Secretary’s ability to establish meaningful best practices and policies with regard to identity management;
3. The industries that design, create and implement ID technology and solutions; and

² www.ISO.org.

4. The American public, who deserve to have the best available technological solutions implemented so as to protect their privacy and also ensure their security.

We recommend that future Draft Reports detail which RF-enabled technologies it may refer to, and provide substantive scientific or field-test data to support its conclusions.

Technology by itself cannot track people; only those who control the data may track people.

Another major concern for AeA is the repeated reference to the “tracking of human beings,” a phrase that seems to only be associated in the Draft Report with the RF-enabled capabilities of remotely-readable credentials. AeA would like to respectfully remind the Subcommittee that technology is neither benign nor malignant, but inherently neutral. It is the intent and practice of the technology *user* that determines how the data culled from the technology itself will be used – whether the technology is RF-based or contact-card based, a one-dimensional bar code system or a two-dimensional bar code system, utilizes a magnetic stripe or an optically-read system. Because all of these systems are machine-readable, they are *all* capable of tracking the credential holder *if* it is the intent and desire of the implementing agency to do so by collecting and saving the information of all those who pass through the system.

Ironically, because a number of remotely readable RF-enabled technologies can accommodate encryption and on-board processing of information, this technology would actually provide *additional protections and security against unauthorized tracking* beyond what is contemplated in the Draft Report. There are a number of reasons why DHS may seek to implement remotely readable identity credentials:

- To ensure the integrity and authenticity of the ID credential against forgery and tampering;
- To authenticate the holder of the ID credential to the credential itself, using biometrics;
- To increase the confidence in the identification process; and
- To increase the speed and efficiency of the identification process.

Because many remotely-readable technologies can have on-board processing directly on the contactless integrated circuit (IC) of the chip, implementing agencies within DHS have a fifth reason to implement a remotely readable ID document: *the credentials can be programmed to choose which readers are authorized to read and/or collect all, some or none of the data contained in the credential.* For example, Homeland Security Presidential Directive 12 (HSPD12) requires each federal agency to implement a biometrically enabled identity card for all employees. Under HSPD12, each agency will be responsible for the access right granted to their employees. However, when an employee from one agency visits another agency, the employee will not automatically be admitted into the agency visited without first

receiving access rights from that agency. In this case the card will not be recognized or read until it is authorized into the system, and certain information may or may not be collected and stored.

Both through technology and best practices, AeA strongly supports safeguards against the surreptitious and unauthorized tracking of individuals. Since strict control over the flow and capture of information can be exerted at the program manager level, the use of remotely-readable RF-enabled identity credentials will actually empower the Department of Homeland Security to fulfill its Congressionally mandated objectives *and* ensure the privacy and security of those to whom it issues remotely-readable identity credentials.

AeA recommends that the final Report to the Secretary convey each appropriate technology's capabilities and limitations in light of each anticipated application or mission. As stated in the Draft Report, when program managers determine that an RF-enabled remotely-readable credential is necessary, then best practices should be in place to guide the implementers on how to protect American's privacy and security. AeA recommends that a thorough analysis of each appropriate technology be taken *in light of the Best Practices and specific mission requirements for each application*. It is inappropriate, however, for the Draft Report to pre-judge or disfavor *any* technology as the report seems to do; it is appropriate, however, to disfavor and even prohibit certain information collection and management *practices* when they fall outside of the program's stated objective.

While AeA finds fault with the conclusory statements made in the open section of Section VI, AeA applauds the Subcommittee on the Best Practices it recommends to the Secretary and offers a rubric from which technology choices and implementations may be made.

For over 60 years, AeA has been on the forefront of advocating the use of technology to protect American's privacy and security, within government, commercial and personal applications. As a matter of fact, AeA was founded in 1943 in order to advise the federal government about advances in technology and its best applications to further governmental needs. We support the Secretary's efforts to use technology wisely to further the Department's critical needs and Congressional mandates, as well as praise the Committee's work to promote best privacy and security practices to reinforce the Secretary's mission. AeA believes that the Draft Reports' reliance on existing best practices, as well as its concerns and recommendations about Notice, Control, Security, Avoiding Mission Creep and Education all should be commended. AeA recommends a methodology from which technology choices can be made, as well as additional best practices that the Committee may find helpful.

All technology choices should flow from a strong privacy and security policy.

Many of the concerns highlighted in the Draft Report flow from a need to protect American citizens' privacy and security – and rightfully so. AeA recommends that prior to choosing any particular technology for an application, a series of considerations be taken into account, in a critical order. The Department of Homeland Security should:

1. Create strong privacy and security best practices and policies for all technology applications;
2. Ensure that each application's mission fits within DHS's best practices and policies; *and then*
3. Choose the appropriate technology.

By following this rubric, AeA is confident that which ever technology DHS chooses to implement will satisfy both the program's mission critical requirements *and* satisfy the Secretary's desire to protect American's privacy and security.

Additional Privacy Policies and Best Practices suggestions.

Personal privacy can be preserved and even increased by the use of secure RF-enabled technologies in identity documents in combination with strong privacy policies and procedures. The following outlines personal data privacy and secure technology best practices to be employed by government entities when choosing RF-enabled technologies for personal identification.

Strong Privacy Policies

Organizations that need to verify identities find that concerns about privacy and the protection of personal information quickly emerge as key issues when considering new identity management systems. An organization's specific requirements for safety and security must be balanced against the genuine desire to protect the privacy of the individuals whose identities need to be verified. In designing identity management systems, government agencies must balance security and privacy by adopting the following privacy principles:

- The organization must have a privacy and security policy that clearly defines what personal information is to be collected, how the information will be used, who can access the information, how the information will be protected, and how the individual will control its use and provide updates to the information over time.
- The enrollment and identity proofing process must verify that the information presented is accurate and protect the confidentiality and integrity of that information.

- The identity management system must protect each individual's information at all times, including while the information is being stored and while it is being used.
- The ID an individual carries must protect its contents from being copied, altered, or hacked, to prevent unauthorized use, misuse, or disclosure of the personal information it carries.
- The exchange of personal identifiable information between the ID and the reading device must be protected to prevent unauthorized capture and use of data to impersonate an individual.
- Access to the personal information should only be granted through an issuer-defined authentication process. Only necessary information should be released and only to authorized systems or individuals.
- All personnel involved in using the system must be carefully trained and monitored to ensure strict conformance to the system's policies, procedures and practices. Compromising these policies, procedures and practices means compromising the identity management system itself.

In addition to the Best Practices noted above and within the Draft Report, the Committee may find these suggestions to be helpful as well:

Privacy Policies – Government agencies implementing identity management systems should conform to the Information Practices Act of 1977.

Public Notification and Education – Government agencies and other entities choosing to employ high security contactless smart cards for identification purposes should notify consumers of data privacy policies and security features in place, including consumer rights to access and notification.

Designing an identity management system to guard individual privacy involves more than simply following general best practices and then selecting a particular type of ID technology. The organization issuing the ID must design information privacy and security into the overall system, have the appropriate policies and processes in place to support the privacy and security requirements, and implement the technologies that deliver these features. Issuing organizations must also have the operational practices in place to monitor and ensure that privacy and security policies are implemented and strictly followed.

RF-enabled Technology Best Practices

The selection of an ID technology is also critical. The ID technology must be one that can both facilitate and reinforce the system's privacy and security design and goals. Contactless integrated circuit

chips represent a significant advance in securing identification technologies, incorporating strong security features that can enhance privacy protection in a well-designed and properly implemented system. Federal agencies should adopt the following best practices in implementing an identity management employing RF-enabled identity credentials and documents:

- *Strong information protection.* Encrypt the identity information stored on the ID and encrypt communications between the ID and the reader device, to prevent eavesdropping when personally identifiable information is on the ID. The remotely-readable ID can also lock the personal information on the ID and release it only after the owner authorizes the release by providing unique information.
- *Security, security, security.* Incorporate tamper-resistant features to prevent duplication and forgery, including as a means to combat identity theft and fraud. The remotely-readable IDs can include a variety of hardware and software capabilities that immediately detect and react to tampering attempts, countering possible attacks.
- *Authenticated and authorized information access.* Require secure access to the credential by enabling the remotely-readable ID to verify the authenticity of the reader and prove its own authenticity to the reader. For example, government agencies can restrict access to certain data on the card by enabling the card itself to verify the authority of the information requestor.

Conclusion

AeA's member companies take consumer privacy and security very seriously and take great steps to ensure that consumer information is both safeguarded and dealt with correctly. As such, we applaud the Secretary's efforts to protect American's privacy and security concerns. We continue to have strong concerns, however, with many of the conclusions drawn about the RF-enabled technologies noted in the Draft Report. AeA is confident, however, that these issues will be addressed in future iterations of the Draft Report, and in the Final Report as it is presented to the Chief Privacy Officer and the Secretary. As it goes forward with the Draft Report, AeA would like to reiterate a sentiment mentioned previously: *Don't ban technology, ban bad behavior.* It is AeA's hope that the Committee develops policies that protect personal privacy and security *first*, and then empower agency implementers to choose the technologies that will fulfill those policies. AeA further hopes that the Final Draft makes it clear that any

conclusions about RF-enabled technologies be advisory for the Department of Homeland Security only, while the Best Practices and Security Policies stated should be considered, and implemented within the Department of Homeland Security.

As such, AeA respectfully requests that the Subcommittee address the concerns stated in this comment paper and include AeA's suggestions on Best Practices and policy recommendations. AeA is committed to working with the Department of Homeland Security in creating a strong policy statement that will protect Americans and help the Secretary's efforts to secure our nation.

We thank you for considering our views, and would be pleased to answer any questions the Commission may have.

Respectfully submitted,

AeA
601 Pennsylvania Avenue
Suite 600, North Building
Washington, D.C. 20004

/s/ Marc-Anthony Signorino

Marc-Anthony Signorino
Director & Counsel, Technology Policy
May 20, 2006

CERTIFICATE OF SERVICE

I, Marc-Anthony J. Signorino, Director and Counsel for Technology Policy for AeA (The American Electronics Association), hereby certify that a true and correct copy of the foregoing Comments of AeA was sent this 20th day of May, 2006, electronically to the Department of Homeland Security via email to PrivacyCommittee@DHS.gov

/s/ Marc-Anthony Signorino .

Marc-Anthony Signorino
Director & Counsel, Technology Policy
AeA