Report No. 2006-02

The Use of RFID for Human Identity Verification

This paper reflects the recommendations provided by the Data Privacy and Integrity Advisory Committee (Committee) to the Secretary and the Chief Privacy Officer of the Department of Homeland Security (DHS). The Committee's charter under the Federal Advisory Committee Act is to provide advice on programmatic, policy, operational, administrative, and technological issues relevant to DHS that affect individual privacy, data integrity and data interoperability and other privacy related issues.

I. Introduction and Executive Summary

The purposes of this paper are to: (1) offer an analytical framework for use by the Department of Homeland Security ("DHS" or "the Department") in determining whether to deploy a Radio Frequency Identification (RFID)-enabled system to identify and/or record the presence of individuals; and (2) offer a set of best practices to consider when DHS chooses to use an RFID-enabled system. The focus of this paper is on such systems in border-crossing contexts. We believe that the issues raised in this paper are relevant to other credential or human-identification related applications, and that the best practices we recommend are also applicable in those contexts.

There is general agreement among industry, government, and privacy advocates that automatic identification technologies such as RFID can have valuable uses, especially in connection with tracking things for purposes such as inventory management. RFID is particularly useful where it can be embedded within an object, such as a shipping container or a document.

There is less agreement among industry, the public, government, and the advocacy community on the appropriateness of using RFID-enabled systems to identify individuals passing a checkpoint. On the one hand, there is the potential for benefits in terms of greater accuracy, speed and efficiency when deploying an RFID-enabled system to identify individuals. Newer RFID credentials may also have added benefits of greater fraud prevention and tamper resistance than existing credentials. This would be the likely case in any new credential, whether RFID or not, but may be considered a collateral benefit of deploying new credentials. Such new technology may also increase both the cost and complexity of using forged documents. Lastly, there may be benefits in tracking lost identity credentials, such as preventing the casual/opportunistic misuse of the credential. However, it does not address issues related to concerted efforts to falsify credentials.

On the other hand, there are a variety of concerns about the use of such systems, including:

- The potential for unauthorized access to the data on the RFID-enabled device, or the data when in transit between the device and reader;
- The selection of RFID-enabled systems for an application if other existing and potentially less privacy-impacting alternatives can achieve the same benefit;
- The concern that the information produced by an RFID-enabled credential system for a stated purpose might be reused or leveraged for a second purpose without the knowledge or consent of those persons whose information was collected for the original purpose;

- The concern that the deployment of RFID-enabled systems represents the potential for widespread surveillance of individuals, including US citizens, without their knowledge or consent.

Before deploying any technology, the Department should define the program objective, determine what technologies may apply, and understand the benefits and concerns related to each deployment. With that as background, there needs to be an analysis of what is the least intrusive technology that can be used to accomplish the objectives of the program and what technologies can be used to help address any privacy concerns that exist.

With specific reference to RFID deployments, we recommend that if the Department, after careful consideration of all technologies and analysis of the least intrusive means to achieve department objectives, determines to deploy an RFID-enabled system to identify individuals, that it build in, from the design stage, sufficient privacy and security safeguards to ensure that the use of RFID-enabled systems meets the Department's objectives while respecting and protecting the privacy and security of information collected about individuals[1] throughout the lifetime of the system and, in the case of the information, beyond.

II. RFID Technology Overview

In order to frame this discussion, we begin by presenting a brief overview of RFID technology. This is not meant to be a complete tutorial discussion, since those may be found elsewhere.[2]

RFID is a type of automatic identification technology that enables the user to "tag" objects with a tiny[3] device that can later be detected by automatic means. That detection can range from simply noting the presence of the device, to obtaining a fixed identification number from the device, to initiating a two-way communication with the device. The essential functionality of the system is that when the tag is in the presence of an appropriate radio frequency (RF) signal emanated by a *reader* the tag responds by sending back a reflected RF signal with information in response. Some can only operate over a very short distance of a few centimeters or less, while others may operate at longer distances of several meters or more. At the higher-end of RF technology, the contactless RFID tags have been enhanced with the full capabilities of smart card chips containing general-purpose computer processors and larger non-volatile memory spaces.

---

[1] Some commentators have suggested that the Committee supplement this paper with a list of the various current and planned uses of RFID by the Department of Homeland Security. The Committee declines to do so for two reasons: first, any such list may soon become incorrect or obsolete; and second, because this paper is intended to serve as a framework for the Department to use in any evaluation of a program that would use an RFID-enabled system to identify individuals.

[2] Garfinkel and Rosenberg, eds., "RFID Applications, Security, and Privacy". *See also* Department of Homeland Security Office of the Inspector General report entitled "Enhanced Security Controls Needed for US-VISIT's System Using RFID Technology (Redacted)". OIG-06-39 (June 2006) at 3-5, available at http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-39_Jun06.pdf. Also see Appendix — Background Materials on RFID Technology.

[3] These are as small as 0.15mm x 0.15mm and thinner than a sheet of paper at 7.5 micrometers. *See* http://www.eetimes.com/news/design/showArticle.jhtml?articleID=179100286 .

RFID tags can be made to respond only to specific readers (or ones implementing specific communication protocols). Today, almost all tags operate at a single or small range of frequencies using a single protocol. Some advanced readers may read more than one protocol but generally only at one frequency.

The tags come in three types: *passive*, *active*, and *semi-active* (or *battery-assisted***)**, each with its own set of operating characteristics.

Passive tags have no battery inside and, thus, must depend upon the current induced in their antennas by the reader's RF signal to perform their jobs. This allows the device itself to be smaller than active tag devices and increases their useful lifetime. Depending upon the technology, these passive tags can return a fixed value, be writable once and then read many times, or may be fully rewritable. Because of their dependence upon the reader's continuous RF signal for power to process and transmit their response, reading passive tags may be somewhat less reliable than reading active or semi-active tags.

Active tags contain their own battery. Once "awakened" by a reader's RF signal, these tags employ their own power to perform their jobs. Other active tags act like beacons that continually emit an identification signal. The advantage of the active tags over the passive is their typically greater computational capability, memory capacity, and the distance over which they may be read. While their batteries do have a limited lifetime, it is typically several years. Since their batteries power their response, active tags are more appropriate in situations where RF signals might encounter interference. Semi-active or battery-assisted tags are simply passive tags that use the tags' batteries to power their electronic circuits rather than depending on power drawn from the field of the reader. As a result, their range is longer than that of passive tags.

High-end, active RFID tags can have rather extensive computational capability. They can provide cryptographic functions to support more secure and private operations, have considerably larger memory capacities, and can enter into complicated communications protocols that could reduce the possibility of unintended communications with unauthorized readers.

One aspect of most RFID tags is that it is quite easy to awaken them with the appropriate RF signal. This implies that the object with which the tag is associated often does not need to do anything to enable this communications link. In the case of shipping containers or livestock, this is a clear advantage. However, this automatic feature has proven controversial in the wide variety of applications of RFID technology around humans.

Today many RFID tags are passive, though a growing numbers are shifting to active or semi-active. Factors in these selections include both functionality and cost. The higher end functions of RFID are still considered costly for broad commercial application. Size is also decreasing, but again the vast majority of tags are still applied to shipping cartons, containers and pallets. To date most RFID deployments are part of the commercial back end, dealing with supply chain and logistics. There is general agreement that many of the current applications such as supply chain/logistics and food safety are beneficial and have little to no negative privacy implication. As costs decrease and item level tagging becomes more feasible, greater penetration of beneficial applications, such as drug safety, warranty/service, product safety and product recall is likely to occur, but those functions may have greater privacy implications. The privacy implications arise from the possibility that the item is

carried by the person and, depending on the tag, technology and configuration, may be observed by other readers.

Where issues arise as to whether RFID may create privacy implications, certain technologies may be applied to limit the potential exposure of Personally-Identifiable Information (PII). These technologies include encryption, kill switches, tearable tags, on/off switches and nonmanufacturer technologies to block, disable, or zap tags. These technologies may be used alone or in combinations to achieve the desired levels of protection and functionality. Each of these functions will, of necessity, increase at least the initial cost of such RFID-enabled deployments. It should also be recognized that these technologies do not operate in a vacuum, but rather operate within the context of various laws and policies, which may further limit the type of information that can be collected or how such information can be used.

IV. The Legal Basis for RFID Use in Human Identification

The major laws, executive orders, and programs under which RFID is being considered or used are either permissive as to technology or not legally binding on the U.S. government.[4] Nevertheless, when an RFID-enabled system is used to collect data about individuals, the data collected will comprise a "system of records" under the Privacy Act of 1974. People should have at least the rights accorded them by that law when they are identified using RFID. Systems using RFID technology are also subject to the E-Government Act's Privacy Impact Assessment requirements.

V. Use of an RFID-Enabled System for Human Identification

A number of DHS programs are premised on the identification of human subjects. At the border, at airports, and at entrances to secure facilities of all kinds, checking identification cards is a routinely used security measure. RFID is a rapid way to read data, but *RFID in a credential merely identifies the credential, not the individual bearing it*. One or more biometric identifiers can be used to improve identification of human beings, but the steps needed to verify the biometric information using today's technology may reduce or negate the speed benefit offered by radio transmission. Earlier identification of a person approaching a point of identification could also provide security benefits if the information has not otherwise been communicated.

A. Controlling Access, Controlling Borders, and Interdicting Suspects

Whether through RFID or other means, checking identification is intended to achieve a number of different goals: Facility managers use identification to control access to sensitive infrastructures that may be damaged or used to harm people. They use it to control access to facilities where sensitive information about other infrastructure may be kept, or where security planning or operations are carried out. The government uses identification administratively to record the border crossings of

[4] The REAL ID Act, about which regulations are still being formulated, calls for a "machine-readable technology" but does not specify the technology. Homeland Security Presidential Directive 12 calls for "a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)." The State Department adopted RFID technology in the e-passport to meet International Civil Aviation Organization standards, which are not legally binding on the U.S. government.

international travelers. At borders and checkpoints, identification can help detect and interdict undesirable entrants to the country and known or suspected terrorists.

These identification processes are intended to protect a wide variety of institutions, infrastructures, processes, and persons from a wide variety of threats, each having a different risk profile. At base, identification checks by DHS seek to interdict potential attackers on our institutions, infrastructure, and people.

B. RFID Technology Can Reduce Delay at Entrances and Checkpoints, But Standing Alone, It Cannot Identify An Individual

It takes some time to check a traditional identification document. The process typically includes handing the document to a verifier, who must review the information on the document and authorize the bearer to pass, record the bearer's passing, or, if appropriate, detain the bearer. The verifier must also compare the identifiers on the document with the bearer to ensure that the bearer is the person identified by the document.

An RFID-chipped identification card can quickly communicate information from the card to a reader at a distance, without a line of sight or physical contact between a card and reader. Transmitting information via radio in advance can thus allow information to be "pre-positioned" before an individual approaches an entrance or checkpoint. While this may improve efficiency at the borders and checkpoints, the verifier must still review authorizing information and compare the identifiers from the card with the bearer in order to ensure that the RFID-enabled card is being carried by the person with whom it is associated. Thus, if the expected primary benefit of deploying RFID is speed and efficiency, care must be taken to ensure that the activities that are necessary to support it do not offset the gains brought by the RFID deployment.

VI. Privacy and Security Issues Associated with the Use of RFID for Human Identification

While RFID-enabled systems may provide at least incremental benefits in terms of efficiency of identification, the use of RFID-enabled systems for human identification may create a number of risks that are not found in conventional identification processes.

A. Potential for Privacy Risks

Digital identification systems pose privacy risks. 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.[5] If not properly protected, this information could also be repeatedly shared or used for secondary purposes, even potentially used for broader surveillance.

[5] At its March 2006 meeting, then-US-VISIT Director Jim Williams testified to this committee that biometric data collected digitally in that program is kept for 75 years, stating "we would not agree to expunge those records." Also, see Wilson P. Dizard III, *E-Passport's First Deployment*, Government Computer News, Oct. 9, 2006 http://www.gcn.com/print/25_30/42249-1.html where he reports that DHS also intends to keep data collected using the E-Passport system for 75 years.

There are particular risks of RFID as the basis for digital identification: (1) Unauthorized readers that enable other people to access the information contained in the RFID (*skimming*); (2) Interception of the transmission of the information by an unauthorized third-party (*eavesdropping*); and (3) if no specific safeguards are put in place, the use of RFID-enabled systems could ultimately aid the monitoring of individuals' movements (*tracking*). While no DHS program plans any secondary use of the data that would create a profile of a person's activities for subsequent, non-security-related use, the potential for misuse remains.

B. The Difficulty with Notice to Subjects of RFID Identification

RFID-tagged identification documents present a significant problem in terms of notice along two dimensions. First, individuals carrying RFID-tagged documents may not always know when they are being identified and to whom, unless people begin carrying radio frequency detectors or purses and wallets that are impermeable to radio frequencies. Second, people with RFID-tagged documents may not always know what information they are sharing when they are identified using an RFID-enabled system. In a visual ID-check environment, people know that only the information on the card is available to a verifier, along with any information linked to that card in databases.

C. Security is a Foremost Concern with Using RFID for Human Identification

Some of the greatest concerns with RFID-enabled systems used to identify individuals have to do with the security of the transmissions from the tags to the readers.

Making identification information available via radio frequency opens up two sources of security risks, commonly known as "skimming" and "eavesdropping." "Skimming" is creating an unauthorized connection with an RFID tag in order to gain access to its data. It allows someone outside of the identification system or program to gather information surreptitiously. This risk can be controlled a number of ways. One is to block the transmission of radio signals to and from the chip when it is not intended to be in use. For example, a Faraday cage or shield is a wire screen that prevents transmission of radio signals. The State Department's new e-passport will incorporate this technology. It is more convenient in a "passbook" type document like a passport than a card for which there would have to be some sort of wrapper or sleeve. This threat may be reduced through the use of some solution with higher functionality.

Another way to limit skimming is to encrypt the data transmission so that identification information appears indecipherable to anyone intercepting it who is not authorized to read it. However, this is not a complete solution. Though indecipherable itself, the encrypted information can act as an identifier if it remains the same each time the card is skimmed, just as a person might be known by a nickname.

"Eavesdropping" is the interception of the electronic communication session between an RFID tag and an authorized reader, again, in order to gain access to the data being transmitted. As with skimming, depending on the design of the system, an eavesdropper may be able to collect usable information from the communication between an RFID chip and an authorized reader even if the communication is encrypted.

One way to suppress eavesdropping is to limit carefully the environments in which identification cards are used. Another is to design the RFID chip so that no two communication sessions appear alike.

In any event, privacy and security must be built into the full lifecycle of the RFID application from the outset – from the design stage, to deployment and use, to end-of-life. Just as privacy concerns must be identified in a broad and systemic manner, so too must technological solutions be addressed systematically.

D. RFID Security Issues Identified by the GAO

The United States Government Accountability Office addressed the use of RFID technology in a May 2005 report titled *Information Security: Radio Frequency Identification Technology in the Federal Government* (GAO Report)[6]. The GAO Report identified a number of security issues that are implicated by federal (and commercial) use of RFID technology. "Without effective security controls," the GAO Report stated, "data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users."[7] The GAO stated that RFID systems should be designed to:

- Ensure that only authorized readers can read the tags, and that only authorized personnel have access to the readers;
- Maintain the integrity of the data on the chip and stored in the database;
- Ensure that the critical data is fully available when necessary;
- Mitigate the risk of various attacks, such as counterfeiting or cloning (when an attacker produces an unauthorized copy of a legitimate tag); replay (when a valid transmission is repeated, either by the originator or an unauthorized person who intercepts it and retransmits it); and eavesdropping;
- Avoid electronic collisions when multiple tags and/or readers are present; and
- Mitigate the likelihood that unauthorized components may interfere or imitate legitimate system components.

The GAO Report maintains that many security risks can be mitigated through compliance with the Federal Information Security Management Act (FISMA), which requires each agency to develop, document, and implement an agency-wide information security program. Specifically, FISMA requires agencies to:

- Engage in periodic risk assessments;
- Develop risk-based policies and procedures to reduce risks to an acceptable level;
- Develop plans for providing adequate information security for networks, facilities, systems, and groups of systems;
- Engage in security training for personnel and contractors;

[6] See GAO-05-551 (May 2005), available at http://www.gao.gov/new.items/d05551.pdf. See also Testimony of Gregory C. Wilshusen, Director, Information Security Issues, Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, House Committee on Homeland Security, June 22, 2005, available at http://www.gao.gov/new.items/d05849t.pdf.

[7] GAO Report at 19.

- Test the information security policies at least annually, including the testing of management, operational, and technical controls for every major information system;
- Develop a process to detect and report security incidents and a remedial action process; and
- Maintain procedures for continuity of operations in light of a security incident.

As it relates to RFID, an agency can reduce the risk of unauthorized use or access through encryption and authentication.

- Encryption should include the data in the tags, in the air, and when stored in a database.
- Authentication means verifying the claimed identity of a user. It can be used between tag and reader as a way to mitigate security risks. This can help prevent the unauthorized reading of and/or writing to tags.

The GAO states that the privacy issues can be mitigated by compliance with existing legislation, including compliance with:

- The Privacy Act of 1974; and
- The Privacy Impact Assessment requirements of the E-Government Act.

The Department of Homeland Security's Office of Inspector General, in its report on the US-VISIT ("The DHS Inspector General's Report")[8], also notes a number of steps that the Department of Homeland Security can take to ensure the security of databases used in RFID-enabled programs. Those recommendations included the development and implementation of procedures to strengthen the password management and user account processes relating to the database associated with an RFID-enabled program.

VII. Recommendations

The case for using RFID-enabled systems to track materiel is clear. The Department of Defense, for example, has produced a significant study showing the benefits of using RFID to tame the substantial logistical challenges it faces.[9] The case for using RFID-enabled systems by the government to identify and record the presence of individuals, however, requires a more careful analysis involving the mission to be accomplished, the alternative technologies available, and the practicability of employing safeguards to protect the privacy and security of information collected from and about individuals.

A. The Decision Whether to Use RFID to Identify Individuals

In light of the concerns associated with the privacy and security of information gathered by means of an RFID-enabled system, the recommendations in the GAO Report and the DHS Inspector General's Report, and in light of comments received by the Committee on the first draft of this paper and the Committee's own deliberations, the Committee recommends that Program Managers within the U.S.

[8] Department of Homeland Security, Office of Inspector General, Enhanced Security Controls Needed For US-VISIT's System Using RFID Technology (June 2006) https://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-39_Jun06.pdf

[9] Final Regulatory Flexibility Analysis of Passive Radio Frequency Identification (RFID), prepared by the Office of the Under Secretary of Defense for Acquisition Technology & Logistics. See full reference in appendix.

Department of Homeland Security, in consultation with the DHS Privacy Office, explore the following issues to determine if an RFID-enabled system to identify individuals is appropriate to meet a given objective, consistent with the Framework for Privacy Analysis of Programs, Technologies, and Applications:[10]

Objective

- What is the specific objective of the program?
- Does an RFID-enabled system meet the objective?
- Does the RFID-enabled system comply with the recommendations contained in the GAO Report and in the DHS Inspector General's Report? If not, are there compelling reasons for this?

Design Considerations

- Does an RFID-enabled system meet the Department's objective in a way that the Department cannot accomplish using other technologies, such as 2D barcodes, contact-required smart cards, optical character recognition, or magnetic stripes?
- Can an RFID-enabled system provide security and/or privacy benefits that other alternatives cannot provide?
- What type of RFID technology is proposed for the program? Are the tags active or passive? What are the frequencies used and read ranges for the devices? After consulting with security experts within the Department and, if necessary, outside of the Department, are the Program Managers and the DHS Privacy Office satisfied that the read ranges are as short as they are claimed to be and as short as possible to accomplish the objective?
- Does the proposed deployment of an RFID-enabled system to identify individuals provide enhanced efficiencies (including the speed of identification)? Are these negated in whole or in part by the need for human intervention or some type of mechanical validation, or by other factors?

Risk Mitigation – Program Implementation Risks

- Does the proposed RFID-enabled system allow for a framework where individuals can be given the choice of whether or not to participate in RFID usage? Under this paradigm, individuals would be informed of the existence of the tags and the type of information that would be collected and then could decide whether to participate in the program or not. If such a framework is not contemplated, is there a legitimate reason why this should not be part of the RFID-enabled program? Will there be an alternative program for those persons who prefer a non-RFID-enabled document, even if it provides fewer advantages or efficiencies?
- Does the RFID-enabled system provide a means of deactivating the RFID functionality? If not, is there a legitimate reason to not have such a mechanism?
- What safeguards are in place to ensure that the data collected will be used only for purposes of meeting the defined objective? In other words, are there adequate protections against unanticipated secondary uses or sharing of the data? The Committee is especially interested

[10] Framework for Privacy Analysis of Programs, Technologies, and Applications, Report No 2006-001 (March 29, 2006), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf

in this question, because extensive collections of data have, in the past, tended to find new, unanticipated uses.

- How is the information maintained in the back-end systems protected? How long will the information in the database be kept? Is the length of time proposed appropriate given the objective at hand? Can the length of time be minimized without undermining the objective?
- Are there end-to-end auditing capabilities built into the system to monitor use and misuse of the information?

Risk Mitigation – Credential Risks

- What kinds of information are carried on the tag? What kinds of information are passed to a database? Is the amount and type of information narrowly tailored to accomplish the Department's objective?
- How is the information on the tag protected (encryption, no personal information is present on the card, etc.)?
- Is the communication with the reader secured? Are there adequate security protections to ensure that only authorized readers can read the tags?
- Does the RFID-enabled system include RF-blocking technology, such as that proposed by the U.S. Department of State for use in its passport jackets? If not, is there a legitimate reason not to have such a mechanism?
- What security safeguards are in place for the associated databases, tags, and transmissions from the tags to the databases? Have the Program Managers consulted with information security experts within the Department and, if necessary and appropriate, outside of the Department, to ensure that the program is adequately protected from skimming, eavesdropping, and other threats to the security and integrity of the system?

Net Effects

- On balance, if the Program Managers, in consultation with the DHS Privacy Office, determine that an RFID-based technology meets a legitimate Department objective, do privacy and security concerns outweigh the incremental benefits gained by using an RFID-enabled system over a system posing fewer privacy and security risks?

B. Proposed Best Practices for Use of RFID by DHS to Identify Individuals

The Committee recommends that if DHS chooses to deploy an RFID-enabled system to identify individuals, DHS should use as many of the following safeguards as possible and appropriate, given the proposed use:[11]

[11] These proposed best practices draw on a number of sources, including the GAO Report, the EPCglobal Guidelines for Electronic Product Codes for Consumer Products (see http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html), and the ARTICLE 29 WORKING PARTY WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY, 10107/05/EN, WP105 (January 19, 2005) (available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf).

Notice – Individuals should know how and why RFID technology is being used, including what information is being collected and by whom. DHS should consider using standardized icons or other images to highlight the existence and use of RFID tags and the placement of readers;

Open Standards – Because RFID-enabled systems can be configured a variety of ways, it is important that the public have access to information about the design standards to which the systems are built. This information should not be limited to their intended uses, but their maximum capabilities should also be specified. Information about the maker of the chip, the integrator, and the provider of the data system should all be made public, to the extent consistent with national security and anti-circumvention concerns, so that the design and integration choices can be assessed by outside observers, auditors, and the affected public.

Choice and Control (Consent) – Where possible, individuals should have the option not to participate in a program involving the use of RFID technology to record their movements, while maintaining the rights and privileges (but perhaps losing the convenience benefits) of other individuals who are participating in a program involving RFID technology. If a national security or other argument weighs against individual control, such an argument should be explicitly stated and the choice be made available to the extent possible. Perhaps under such circumstances, a notice and comment approach would be appropriate.

Securing Readers and Data – To mitigate eavesdropping and skimming, DHS should ensure that only authorized readers can receive signals from DHS-authorized RFID tags. Data should be encrypted on tags, in transit, and in the database. DHS should limit carefully the environments in which identification cards are used, and design the RFID chip so that no two-communication sessions appear alike. As with any database program, DHS should take all appropriate steps to assure the security and integrity of the database itself. Overall, DHS should follow the security recommendations laid out in the GAO Report, including conducting a FISMA review of the program, as well as recommendations of the department's Office of the Inspector General.

Avoid Function Creep – DHS should use data collected by RFID technology only for the stated objective. It should keep data for only as long as necessary to meet the original objective for which it was collected.

Education Campaign – RFID technology is not well understood by much of the public. Government entities and the private sector often also lack a good understanding of how RFID technologies work and when and how they are best applied. As a result, there are many people for whom the use of RFID technology in identity systems is troubling. Most of their concerns could be easily resolved through education and openness. If it uses RFID, DHS should engage in an education campaign regarding the use of RFID, including why it is necessary and what rights and protections are afforded to individuals.

VIII. Conclusion

The Committee recommends that the Department of Homeland Security carefully weigh the considerations detailed in Section VII of this Report before deciding to deploy an RFID-enabled system to identify individuals. An RFID-enabled system should be secure, narrowly-tailored to

effectively accomplish a Department objective, and the least intrusive to privacy and security in light of alternative technologies to accomplish that objective. Otherwise, the use of RFID, standing alone, may not be best suited for purposes of identifying individuals and other solutions should be considered. The Committee further recommends that if the Department determines to deploy an RFID-enabled system to identify individuals, that it build in, from the design stage, the safeguards outlined in Section VII of this Report to the extent possible to ensure that the use of RFID-enabled systems advance the Department's mission objectives while respecting and protecting the privacy and security of information collected about individuals.

Appendix — Background Materials on RFID Technology

INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT, GAO-05-551 (May 2005), available at http://www.gao.gov/new.items/d05551.pdf

RADIO FREQUENCY IDENTIFICATION: OPPORTUNITIES AND CHALLENGES IN IMPLEMENTATION, DEPARTMENT OF COMMERCE (April 2005), available at http://www.technology.gov/reports/2005/RFID_April.doc

FINAL REGULATORY FLEXIBILITY ANALYSIS OF PASSIVE RADIO FREQUENCY IDENTIFICATION (RFID), prepared by the Office of the Under Secretary of Defense for Acquisition Technology & Logistics, available at http://www.acq.osd.mil/log/rfid/EA_08_02_05_UnHighlighted_Changes.pdf

RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS, A WORKSHOP REPORT FROM THE STAFF OF THE FEDERAL TRADE COMMISSION (March 2005), available at http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

RFID: APPLICATIONS, SECURITY, AND PRIVACY (Simson Garfinkel and Beth Rosenberg, Editors) (2006);

ARTICLE 29 WORKING PARTY WORKING DOCUMENT ON DATA PROTECTION ISSUES RELATED TO RFID TECHNOLOGY, 10107/05/EN, WP105 (January 19, 2005), available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

CDT WORKING GROUP SET OF BEST PRACTICES FOR THE COMMERCIAL USE OF RFID, May 1, 2006, available at http://www.cdt.org/privacy/20060501rfid-best-practices.php. Note that this paper deals largely with the commercial use of RFID, as opposed to the use of RFID by the government, the Committee is grateful to have received two sets of written comments by the CDT on this paper, and has taken those comments into account in drafting this paper.

PRIVACY GUIDELINES FOR RFID INFORMATION SYSTEMS, prepared by Ann Cavoukian, Ph.D., Information and Privacy Commissioner/Ontario, June 2006, available at http://www.ipc.on.ca/docs/rfidgdlines.pdf.