DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)

Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-06-53 **July 2006**

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 27, 2006

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibility to promote economy, efficiency, and effectiveness within the department.

This report assesses the strengths and weaknesses of controls over systems using Radio Frequency Identification (RFID) at DHS. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, technical scans, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

AIDMS	Automated Identification Management System
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
FAST	Free and Secure Trade
GAO	Government Accountability Office
Gen2	Generation 2
GES	Global Enrollment System
OIG	Office of Inspector General
RFID	Radio Frequency Identification
S&T	Science and Technology
TSA	Transportation Security Administration
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
WMO	Wireless Management Office

Executive Summary

We audited the Department of Homeland Security (DHS) and its organizational components to evaluate the effectiveness of controls implemented or planned on systems using Radio Frequency Identification (RFID) technology. Further, for systems utilizing RFID technology that were in the planning stages, we determined whether security controls were adequately addressed during the system development process.

RFID is a wireless technology that stores and retrieves data remotely from devices. Systems employing RFID technology include tags and readers on the front end and applications and databases on the back end. The technology allows sensitive information to be read and written to tags and for numerous tags to be scanned simultaneously from a distance. The flexibility and portability of RFID technology and devices, as well as the information that resides on the tags, increase the need for security and privacy controls.

We performed our audit at four DHS organizational components: Science and Technology (S&T), Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. Our results were summarized in separate reports with findings and recommendations issued to CBP, TSA, and US-VISIT. No report was issued to S&T as its efforts in RFID involved only systems in the early stages of development.

CBP, TSA, and US-VISIT have implemented effective physical security controls over RFID tags, readers, computer equipment, and databases supporting the RFID systems at the sites visited. No personal information is stored on the tags. Sensitive information is maintained in and can be obtained only with access to the system's database. Additional security controls would be required if any component decides to store sensitive or personal information on RFID tags or migrates to universally readable Generation 2 (Gen2) products.

Overall, good physical security controls exist on the RFID systems we audited. However, there remain other concerns that should be addressed to help improve system security. DHS needs to develop policy and procedures regarding RFID technology, incorporating security planning

while in system development, and strengthen database security controls. These security-related concerns, if not addressed, increase the potential for unauthorized access to DHS resources and data.

The DHS Chief Information Officer (CIO) has not developed department-wide policies and guidance regarding the management and protection of RFID systems. Further, none of the four components reviewed has developed its own RFID policies in order to protect their RFID systems. In addition, operating procedures for RFID systems at CBP and US-VISIT, including physical security of unused tags and proper destruction of damaged tags, were either incomplete or not followed consistently.

CBP, TSA, and US-VISIT need to determine whether the necessary database security controls are being implemented in their RFID systems. Our vulnerability assessments of two CBP systems (Global Enrollment System (GES) and Free and Secure Trade (FAST)) as well as US-VISIT's Automated Identification Management System (AIDMS) identified security concerns with user account and password management, user access permissions, and auditing. In addition, system configuration weaknesses exist with TSA's weapons management system, and finally, the systems at CBP and TSA lacked accreditation. We identified similar issues in other DHS components' database systems in our December 2005 report, *Security Weaknesses Increase Risk to Critical DHS Databases*. Processes need to be put in place at the department level to ensure that database security concerns at all DHS components are addressed and mitigated.

We are recommending that the DHS CIO:

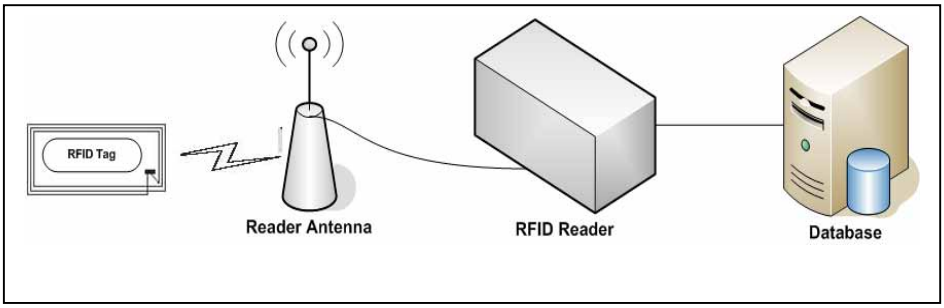
- Develop and implement policy and guidance that addresses security controls for systems being implemented using RFID technology.
- Direct the DHS RFID Coordination Group to finalize its charter and ensure that all components using or planning to use RFID technologies are represented in the group.
- Ensure that components adhere to DHS information security procedures (that is, perform vulnerability assessments and review user access at least annually) for all systems using RFID technology.

In response to our draft report, DHS agreed and plans to take steps to implement each of the recommendations. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

RFID is a wireless technology that stores and retrieves data remotely on devices called RFID tags. RFID can be used almost anywhere -- from clothing tags to missiles. Technology components of an RFID system consist of a tag, reader, and database (see Figure 1).

Figure 1: Components of an RFID System



In a typical RFID system, individual objects are equipped with a small, inexpensive tag that contains a transponder with a digital memory chip and a unique electronic product code. The RFID reader, which is an antenna packaged with a transceiver and decoder, emits a signal activating the tag so it can read and write data to the tag. The reader decodes the data in the tag's integrated circuit, and that data is then passed to a host computer's database for processing.

The tags are small objects that can be attached to or incorporated into a product, much like the standard bar codes on products in the supermarket. The difference is that while it takes a laser to scan a standard bar code and read its information, an RFID tag stores its identifying code on a tiny microchip and transmits it wirelessly to a reader device. RFID technology allows more tags to be scanned simultaneously from a greater distance, and it allows individual items - not just types of items - to be assigned unique identifying codes. There are three types of tags in use today:

- Active tags can store large amounts of information using a power source within the tag.
- Passive tags do not use a separate external power source but rather obtain operating power from the tag reader.
- Semi-passive tags use an internal power source to monitor environmental conditions, and require radio frequency energy transferred from the reader to power a tag's response (similar to passive tags).

Generation 1 tags use proprietary technology, which means that if Company A puts an RFID tag on a product it cannot be read by Company B unless both use the same RFID system supplied from the same vendor. In addition, a new RFID standard, Gen2, was ratified in December 2004 by the RFID international standards organization EPCglobal. The purpose of the Gen2 standard is to improve the interoperability among different RFID products and systems from various manufacturers and different frequencies used in different countries worldwide. Gen2 compliant products feature enhanced security controls, too.

There are four main frequencies used for RFID systems: low, high, ultrahigh, and microwave. Generally, the higher the frequency, the greater the distance from which tags can be read. See Appendix C for a summary of the typical characteristics of RFID tags and the operating frequencies for passive tags.

The use of RFID technology has introduced new security risks to agency systems. The flexibility and portability of RFID technology and devices increase the need for security. Without effective security controls, data on a 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 system databases can be accessed by unauthorized users. In addition, a May 2005 Government Accountability Office (GAO) report raised privacy concerns related to the use of tags and databases. Among the privacy issues is notifying individuals of the existence or use of the technology.[1]

The DHS Wireless Management Office (WMO) was established within the DHS Office of the CIO to coordinate the development of policy and strategy for the use of wireless technologies across the department. One of its objectives is to identify emerging technologies such as RFID. The DHS RFID Coordination Group was formed under the leadership of the WMO in October 2005. The group serves as a forum for DHS components implementing RFID projects or interested in using RFID technologies.

At the start of our review, DHS did not have an accurate inventory of systems using RFID technology. Therefore, we issued a data call to the Information Systems Security Managers at 12 components to determine the extent that RFID is used at DHS. Most of the DHS components do not have any production systems utilizing RFID. Only CBP (starting in 2002)

[1] *Radio Frequency Identification Technology in the Federal Government* (GAO-05-551, May 2005).

and US-VISIT (starting in 2005) have mission critical systems utilizing RFID. Other components such as S&T and TSA are testing RFID technology with systems under development.

Results of Audit

RFID Policy and Guidance Have Not Been Developed

DHS has not developed a department-wide RFID policy or guidance to provide direction to the components regarding the management and protection of systems using this technology. In addition, none of the four components reviewed (CBP, S&T, TSA, and US-VISIT) have developed their own RFID policies. Further, operating procedures for RFID systems at CBP and US-VISIT were either incomplete or not followed consistently. Without specific RFID policy and procedures, DHS cannot ensure that effective controls are put into practice at all components using this technology.

DHS issued its Sensitive Systems Policy Publication 4300A (DHS Policy) and its companion, DHS Sensitive Systems Handbook (DHS Handbook), to provide direction to its components regarding the management and protection of sensitive systems, including wireless communication technologies and devices. Additionally, the policy outlines management, operational, and technical controls necessary to ensure confidentiality, integrity, availability, and authenticity within the DHS information technology infrastructure and operations.

The WMO is in the process of developing the DHS Information Technology Security Program Handbook for Sensitive Wireless Systems (DHS Wireless Handbook). This handbook will be issued as implementation guidance to address security and countermeasures that can be applied to sensitive wireless systems. In addition, the WMO is currently developing an RFID implementation guide.

The DHS Policy, DHS Handbook, and draft DHS Wireless Handbook do not have specific policy or guidance to address RFID technologies. RFID policies are needed to define the acceptable use of the technology and ensure that adequate controls are implemented to mitigate the risks associated with its use. For example, DHS' wireless policy does not specify the controls needed to mitigate vulnerabilities that are susceptible

to RFID technology, such as counterfeiting or cloning,[2] replay,[3] and eavesdropping. The policy should specify that only authorized RFID readers can read and process the information from the tag, and ensure that data stored on the tag is protected from unauthorized modification.

The WMO drafted a charter for the RFID Coordination Group in December 2005. Included in the mission of the coordination group, as stated in the draft charter, is establishing department-wide polices to procure and implement RFID systems, and to compile best practices and lessons learned in areas such as RFID system architecture, standards, and security. According to the draft charter, the members of the group should be project managers, technical representatives, and other members from DHS components, including the DHS Privacy Office, who are implementing RFID projects or who are interested in using RFID technologies. However, attendance at the meetings has been minimal - limited to WMO personnel and irregular attendance from representatives from DHS Asset Management, S&T, TSA, and US-VISIT. Although CBP has RFID systems in production, no representatives have attended any of the meetings.

CBP developed operating procedures for its systems using RFID. However, it did not address all aspects of RFID technology, such as physical security of unused RFID-enabled cards and the proper destruction of damaged RFID-enabled cards. In addition, procedures for the destruction of RFID-enabled forms that were issued by US-VISIT headquarters to the ports of entry using RFID were not followed consistently.

Issuing a sound RFID policy and guidance is the first step in ensuring that adequate security controls are implemented across the department to protect systems employing the technology or mitigating the risks associated with the use of RFID. Since the department is considering a common RFID standard for all border crossing identification cards, issuing department-wide policy and guidance is needed to help ensure that consistent standards and controls are implemented. Furthermore, RFID systems operating without required security management practices increase the possibility that security controls protecting DHS systems can be circumvented. In addition, a department-wide working group with representation from all components is needed to assist the department in

[2] Cloning an RFID tag occurs when an attacker produces an unauthorized copy of a legitimate tag.
[3] A replay is an attack when a legitimate data transmission is fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it.

developing and implementing RFID policy, guidance, standards, and best practices.

Security Needs To Be Incorporated in the Development of All RFID Systems

Security controls are not integrated into all RFID systems that are currently under development within DHS. To be most effective, security controls must be addressed during the system development process. Without integrating security controls in the system development process, there is little assurance that adequate security will be incorporated into systems using RFID technology once they become operational.

Currently, S&T has systems under development on behalf of TSA and CBP that may employ RFID technology. However, security is not always incorporated when developing the RFID systems. Specifically:

- Testing of security features was not included in the scope of TSA's feasibility evaluation to manage and track both domestic and international cargo and passenger baggage.
- Detailed security requirements were not specified in S&T's proposal to contractors to develop a secure carton system for CBP, as it only required that the cartons have an active RFID chip and be secure.

The National Institute of Standards and Technology requires that security controls be fully documented. Furthermore, the security controls developed for a new information system must be tested and evaluated prior to deployment to ensure that the controls are working properly and are effective. In addition, DHS policy requires that security be integrated into the Systems Development Life Cycle, which includes the planning, requirements definition, design, development, test, and implementation phases. Without considering and incorporating security controls during all phases of a project's development, there is no assurance that all required security features will be considered prior to a system becoming operational.

Security Controls Need Strengthening

DHS needs to strengthen controls over the systems that support RFID technology. We identified vulnerabilities on databases that could be exploited to gain unauthorized or undetected access to sensitive data. We

identified similar issues in other DHS database systems in our December 2005 report, and recommended that the CIO ensure that components adhere to DHS information security procedures.[4] Adequate security procedures for all DHS databases are needed to ensure that data captured and stored is properly protected.

We performed vulnerability assessments and reviewed configuration settings on databases supporting CBP (GES, FAST) and US-VISIT (AIDMS) systems using RFID technology. Security improvements are needed to address areas such as user account and password management, user access permissions, and auditing.

We identified vulnerabilities at CBP and US-VISIT relating to password administration, user access permissions, and auditing. [redacted] Also, we identified additional vulnerabilities at CBP relating to user account and password management. [redacted]

Our review of TSA's security configuration for its weapons management system identified system configuration weaknesses, including [redacted] We noted that systems at CBP and TSA lacked an accreditation to operate, too.

These weaknesses are an indication that user accounts and passwords may not be effective to control access to DHS sensitive data. In addition, [redacted]

The *Federal Information Security Management Act* requires federal agencies to perform periodic testing to evaluate the effectiveness of security controls. Office of Management and Budget Circular A-130 Appendix III requires federal agencies to provide adequate security to their systems and restrict access to authorized users only. Without

[4] *Security Weaknesses Increase Risk to Critical DHS Databases* (OIG-06-17, December 2005).

adequate procedures to ensure that all material vulnerabilities are identified and reviewed, management cannot make certain that data in its critical systems is secure. At the completion of our assessments, we issued technical reports to CBP and US-VISIT detailing the specific vulnerabilities detected on their databases and the actions needed for remediation.

Recommendations

We recommend that the DHS CIO:

1. Develop and implement policy and guidance that addresses security controls for systems being implemented using RFID technology; and ensure that policies and guidance are distributed to all components.
2. Direct the DHS RFID Coordination Group to finalize its charter, and ensure that all components using and planning to use RFID technologies are represented in the group.
3. Ensure that components adhere to the DHS information security procedures, such as perform vulnerability assessments and review user access at least annually, for all systems using RFID technology.

Management Comments and OIG Analysis

DHS agreed with recommendation 1. DHS plans to revise its DHS Policy and DHS Handbook to address RFID technology by October 2, 2006.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS agreed with recommendation 2. The DHS RFID Coordination Group will finalize its charter and include all components using or planning to use RFID technologies by September 30, 2006.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS agreed with recommendation 3. DHS plans to modify its certification and accreditation methodology to incorporate improved vulnerability assessments. In addition, DHS plans to improve procedures over user access reviews by September 30, 2006.

We agree that the steps DHS plans to take begin to satisfy this recommendation.

Purpose, Scope, and Methodology

Our objective was to determine whether DHS and its components have implemented effective controls to protect critical data processed by its RFID systems from unauthorized access. Specifically, we determined whether: (1) DHS and its components developed adequate policies and procedures to ensure the confidentiality, integrity, and availability of data contained on its RFID systems; (2) adequate physical and logical security controls are implemented on its RFID systems; (3) controls implemented to protect the privacy of personal data collected and processed by RFID devices were adequate; and, (4) systems using RFID technology are in compliance with *Federal Information Security Management Act* requirements.

To accomplish our audit, we conducted fieldwork at the following components: CBP, S&T, TSA, and US-VISIT. We interviewed personnel at the Office of the CIO and the components. In addition, we reviewed and evaluated DHS and component security policies, procedures, and other appropriate documentation.

During the audit, we reviewed database settings and used a software tool (Internet Security Systems' Database Scanner) to detect and analyze vulnerabilities on database servers. Also, we used two RFID tools (spectrum analyzer and card reader) to attempt to gain information about the RFID usage at the ports of entry.

We conducted our audit between November 2005 and February 2006 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix D.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General, Office of Information Technology at (202) 254-4100 and Edward G. Coleman, Director, Information Security Audits Division at (202) 254-5444.

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 14, 2006

MEMORANDUM FOR Richard Skinner
Inspector General

FROM: Charles R. Armstrong
Deputy Chief Information Officer

SUBJECT: Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS

We have reviewed your subject report and concur with the findings contained within your final audit report.

Finding and OIG Recommendation No. 1:
"We recommend that the DHS CIO develop and implement policy and guidance that addresses security controls for systems being implemented using RFID technology; and ensure that policies and guidance are distributed to all components."

DHS CIO Management Response:
We accept this finding, and the recommendation will be addressed through the POA&M process. We will implement the recommendation by revising the DHS Sensitive Systems Policy and Sensitive Systems Handbook with a scheduled completion data of October 2, 2006.

Finding and OIG Recommendation No.2
"We recommend that the DHS CIO direct the DHS RFID Coordination Group to finalize its charter, and ensure that all components using and planning to use RFID technologies are represented in the group.

DHS CIO Management Response:
We accept this finding, and the recommendation will be addressed through the POA&M process. The Department CIO will direct the RFID Coordination Group to finalize its charter and include all components planning on using RFID technologies with a completion date of September 30, 2006

Finding and OIG Recommendation No. 3
"We recommend that the DHS CIO ensure that components adhere to the DHS information security procedures, such as perform vulnerability assessments and review user access at least annually, for all systems using RFID technology."

DHS CIO Management Response:
The need to improve vulnerability assessments will be addressed by modification of the DHS C&A methodology to better address the continuous monitoring requirements of NIST 800-37. A POA&M for doing this will be developed in the first Quarter of Fiscal &ear 2007. Based on the experience of other agencies, it may take several years to fully implement the specific requirements of 800-37 with respect to Configuration Management Control, Security Control Monitoring, and Status Reporting and Documentation.

This recommended review of user access is very similar to a previous OIG recommendation, i.e., OIG-05-03, *DHS Needs to Strengthen Controls for Remote Access to Its Systems and Data,* recommendation #2, "Ensure that procedures for granting, monitoring, and removing user access are fully implemented according to DHS requirements, as well as NIST and FISCAM guidelines." Corrective action for reviewing user access is currently specified in the DHS POA&M (weakness #37). The scheduled completion date of July 3 has slipped, and the revised completion data is September 30.

Typical Characteristics of RFID Tags			
Types of Tags	**Power Supply**	**Read Range**	**Type of Memory**
Active	Internal battery	Up to 750 feet	Read-write
Semi-passive	Internal battery	Up to 100 feet	Read-write
Passive	External (from reader)	Up to 20 feet	Mostly read-only

Common RFID Operating Frequencies for Passive Tags			
Frequency		**Typical read range and rate**	**Examples of use**
Low frequency	125 KHz	1.5 feet; low reading speed	Access control, animal tracking, point of sale application.
High frequency	13.56 MHz	3 feet; medium reading speed	Access control, smart cards, item level tracking.
Ultrahigh frequency	860-930 MHz	Up to 15 feet; high reading speed	Pallet tracking, supply chain management.
Microwave frequency	2.45/5.8 GHz	3 feet; high reading speed	Supply chain management.

Information Security Audits Division

Edward G. Coleman, Director
Jeff Arman, Audit Manager
Chiu-Tong Tsang, Audit Team Leader
Charles Twitty, Auditor
Swati Mahajan, Information Technology Specialist
Sharell Matthews, Referencer

Advanced Technology Division

Lane Melton, Senior Security Engineer
Michael Goodman, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Under Secretary, Management
Assistant Secretary, Legislative and Intergovernmental Affairs
Assistant Secretary, Policy
Assistant Secretary, Public Affairs
Chief Information Officer
Chief Information Security Officer
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program, Office of CIO
Chief Information Officer Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.