

# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

### Enhanced Security Controls Needed For US-VISIT's System Using RFID Technology (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552(b)(2). A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-06-39

June 2006

*Office of Inspector General*

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



**Homeland  
Security**

June 16, 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 by our office as part of our oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report assesses the strengths and weaknesses of controls over systems using Radio Frequency Identification (RFID) at the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. 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.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General

# Table of Contents/Abbreviations

---

Executive Summary .....	1
Background .....	3
Results of Audit.....	5
Enhanced Security Controls are Needed to Limit Unauthorized Access to the AIDMS Database .....	5
Recommendations.....	7
Management Comments and OIG Analysis .....	8
RFID Policy and Procedures Not Developed and Issued .....	8
Recommendation .....	9
Management Comments and OIG Analysis .....	9
AIDMS Contingency Plan .....	10
Recommendation .....	10
Management Comments and OIG Analysis .....	11

## Appendices

Appendix A: Purpose, Scope, and Methodology .....	12
Appendix B: Management Response To Draft Report .....	13
Appendix C: Types of RFID Tags and Common RFID Operating Frequencies .....	17
Appendix D: Photographs of US-VISIT Entry and Exit Lanes .....	18
Appendix E: Example of an RFID-enabled Form I-94 .....	19
Appendix F: AIDMS Topology.....	20
Appendix G: Major Contributors to this Report .....	21
Appendix H: Report Distribution.....	22

## Abbreviations

AIDMS	Automated Identification Management System
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
DHS	Department of Homeland Security
DML	Device Management Layer
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
Gen2	Generation 2

# Table of Contents/Abbreviations

---

OIG	Office of Inspector General
POE	Port of Entry
RFID	Radio Frequency Identification
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

# OIG

*Department of Homeland Security  
Office of Inspector General*

---

## Executive Summary

We audited the Department of Homeland Security (DHS) and select organizational components' security programs to evaluate the effectiveness of controls implemented on Radio Frequency Identification (RFID) systems. Systems employing RFID technology include a tag and reader on the front end and an application and database on the back end.

RFID is a wireless technology that stores and retrieves data remotely from devices. The technology allows sensitive information to be read and written to tags and for numerous tags to be scanned simultaneously from a greater 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.

Our objective was to determine whether the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program has implemented effective controls to protect critical data processed by its RFID system from unauthorized access. To address our objective we: (1) interviewed US-VISIT's technical staff; (2) reviewed applicable DHS and US-VISIT policies and procedures; (3) conducted vulnerability assessments of the databases and servers that collect and process information; and (4) evaluated the effectiveness of physical security and assessed the security controls over the RFID-enabled Form I-94s and readers at selected ports of entry (POEs) in [REDACTED] and [REDACTED].<sup>1</sup>

Overall, information security controls have been implemented to provide an effective level of security on the Automated Identification Management System (AIDMS). US-VISIT has implemented effective physical security controls over the RFID tags, readers, computer equipment, and database supporting the RFID system at the POEs visited. No personal information is stored on the tags used for US-VISIT. Travelers' personal information is maintained in and can be obtained only with access to the system's database. Additional security controls would need to be implemented if US-VISIT decides to store travelers' personal information on

---

<sup>1</sup> Form I-94, Arrival-Departure Record, issued at the POE, records the visitor's biographic information; date the visitor arrived in the U.S., and the date when the authorized period of stay expires.

---

RFID-enabled forms or migrates to universally readable Generation 2 (Gen2) products.

Although these controls provide overall system security, US-VISIT has not properly configured its AIDMS database to ensure that data captured and stored is properly protected. Furthermore, while AIDMS is operating with an Authority to Operate, US-VISIT had not tested its contingency plan to ensure that critical operations could be restored in the event of a disruption. In addition, US-VISIT has not developed its own RFID policy or ensured that the standard operating procedures are properly distributed and followed at all POEs.

Subsequent to the completion of our audit work, US-VISIT personnel stated that they had taken or planned to take corrective action to address the vulnerabilities identified during our vulnerability assessment. As fieldwork had already been completed, we did not verify that the vulnerabilities had been remedied.

For systems utilizing RFID technology, we are recommending that the Director, US-VISIT direct its Chief Information Officer (CIO) to:

- Develop and implement procedures to strengthen user account and password management processes relating to the AIDMS database. Procedures should include periodic vulnerability assessments and reviews of all user access.
- Ensure that all vulnerabilities identified for which risks have not been assumed be remedied.
- [REDACTED]
- Test contingency plans, at least annually.
- Develop and implement its own policy that addresses security controls over all components of an RFID system and ensures that policies and procedures are being followed at all affected POEs.

Fieldwork was conducted from November 2005 through February 2006 at selected locations. See Appendix A for our purpose, scope, and methodology.

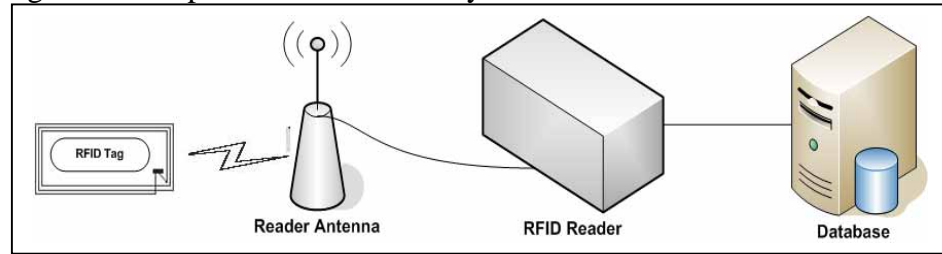
In response to our draft report, US-VISIT agreed and has already taken steps to implement each of the recommendations. US-VISIT's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

---

## Background

RFID is a wireless technology that stores and retrieves data remotely from 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 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 or 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 code tags 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. They obtain operating power from the tag reader.
- Semi-passive tags use an internal power source to monitor environmental conditions, but 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.<sup>2</sup>

US-VISIT is a program established by DHS to: (1) implement an integrated entry and exit data system to record travelers' arrival to and departure from the U.S.; (2) verify the identity of travelers; and (3) confirm the travelers' compliance with the terms of admission to the United States. Currently, US-VISIT is testing RFID technology as a proof of concept to verify that RFID technology best satisfies its requirements of the program at five land POEs: Alexandria Bay, NY; Nogales East and West, AZ; and the Peace Arch and Pacific Highway sites in Blaine, WA. The test began in August 2005. If successful, RFID will be deployed to the 50 busiest land ports by December 31, 2007.

The purpose of US-VISIT's RFID testing is to evaluate the capability to record automatically, passively, and remotely the entry and exit of selected travelers with RFID tags that are embedded in the Form I-94s. US-VISIT has created a new automated system, AIDMS, to link the unique and

---

<sup>2</sup> *Radio Frequency Identification Technology in the Federal Government* (GAO-05-551, May 2005).



---

individually-assigned RFID tag number to existing biographic information received from the Treasury Enforcement Communication System as well as the entry and exit event information for each covered individual crossing a land border.<sup>3</sup> A centralized AIDMS database is located in a secure data center in Ashburn, VA, and Device Management Layer (DML) servers are located [REDACTED]<sup>4</sup>

A unique ID number is embedded in the RFID tag, which associates the I-94 holders with the tag. After the RFID-enabled I-94 is issued to an individual, the unique tag ID number will be used as a record identifier to retrieve individual travelers' biographic information that is stored in other law enforcement databases. When the traveler passes through the entry and exit lanes at a POE, the RFID tag ID number will be read and used to retrieve the traveler's immigration information for use in the inspection processes by U.S. Customs and Border Protection (CBP) officers.<sup>5</sup> As of December 31, 2005, US-VISIT issued 149,414 RFID-enabled Form I-94s to travelers (See Appendix E for an example of RFID-enabled Form I-94, and Appendix F for AIDMS topology).

DHS issued policy and procedures in its DHS 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. Additionally, the policy outlines management, operational, and technical controls including wireless communications, identification, authorization, and access controls necessary to ensure confidentiality, integrity, availability, and authenticity within the DHS information technology infrastructure and operations. DHS has not developed a specific policy associated with the use of RFID technology.

## Results of Audit

### Enhanced Security Controls are Needed to Limit Unauthorized Access to the AIDMS Database

US-VISIT needs to enhance its security controls over the AIDMS database. We performed vulnerability assessments on the AIDMS database and selected DML servers located at [REDACTED]

---

<sup>3</sup> AIDMS is a new system and is separate from the other databases used in the US-VISIT process.

<sup>4</sup> DML servers are used to transmit RFID information captured from the tags at the POEs to the centralized AIDMS database.

<sup>5</sup> Appendix D contains photographs of US-VISIT entry and exit lanes.

---

-----; to evaluate the effectiveness of security controls implemented. In addition, we evaluated the physical security over RFID-enabled Form I-94s, RFID readers, and computer equipment; and tested for wireless signals at selected POEs -----

Overall, information security controls have been implemented to provide an effective level of security on the AIDMS. US-VISIT is ensuring that effective physical controls were implemented over the RFID tags, readers, computer equipment, and database supporting the RFID portion of the US-VISIT program at the sites visited. We used two easily obtainable RFID readers to assess whether unauthorized users could obtain information stored on the tags.<sup>6</sup> We were unable to communicate or read the Form I-94s at the POEs visited. However, when we performed additional testing in a laboratory environment with a more sophisticated reader,<sup>7</sup> we were able to read and verify that only the unique identification number was on the Form I-94. While data on the RFID-enabled Form I-94s are not encrypted and could be subject to interception, RFID tags on the Form I-94s contain no personal information and can be used only to obtain travelers' personal information when combined with the data stored in the AIDMS database. US-VISIT has no plans to store personal data on the tag. Additional controls should be implemented if US-VISIT decides to store travelers' personal information on the RFID-enabled Form I-94 or migrate to universally readable Gen2 products.

During our vulnerability assessment on selected DML servers, we discovered no high or medium security vulnerabilities. However, our assessment results on the AIDMS database revealed some security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data. Specifically, we identified deficiencies in user account and password management, user access permissions, -----  
For example, our vulnerability assessment on the AIDMS database identified the following:

- -----  
-----  
-----  
-----  
-----

---

6 -----  
7 -----

- 
- [Redacted]
  - [Redacted]
  - [Redacted]

Subsequent to the completion of our audit work, US-VISIT personnel stated that they had taken or planned to take corrective action to address the vulnerabilities identified during our vulnerability assessment. As fieldwork had already been completed, we did not verify that the vulnerabilities had been remedied.

Passwords are important - they are often the first line of defense against hackers or insiders who try to obtain unauthorized access to a computer system. Weaknesses in user accounts and passwords may result in inappropriate access to US-VISIT's sensitive data. Unauthorized access to the AIDMS database could occur due to inappropriate user and password settings. Periodic reviews of security settings would identify security weaknesses in user and password management. In addition, without prompt and appropriate review and responses to security events or incidents, violations could occur continuously and cause damage to an entity's resources without detection. As a result, increased risks exist that the US-VISIT may not detect unauthorized activity or determine the users who are responsible.

### **Recommendations**

We recommend that the Director, US-VISIT, direct its CIO to:

1. Develop and implement procedures to strengthen user account and password management processes relating to the AIDMS database. Procedures should include periodic vulnerability assessments and reviews of all user access.
2. Ensure that all vulnerabilities identified for which risks have not been assumed be remedied.

---

3. [REDACTED]

### **Management Comments and OIG Analysis**

US-VISIT agreed with recommendation 1. US-VISIT has implemented procedures to strengthen its account management process and plans to perform vulnerability scans on AIDMS periodically. US-VISIT may delay the development of some account management procedures until the proof of concept testing is completed on AIDMS.

We agree that the steps that US-VISIT has taken, and plans to take, begin to satisfy this recommendation.

US-VISIT agreed with recommendation 2. US-VISIT has taken actions to mitigate the vulnerabilities identified. Corrective action plans have been developed to mitigate and monitor the progress of the remaining vulnerabilities identified for which risks have not been assumed.

We agree that the steps that US-VISIT has taken, and plans to take, begin to satisfy this recommendation.

US-VISIT agreed with recommendation 3. US-VISIT is in the process of developing procedures for [REDACTED].

We agree that the steps that US-VISIT has taken, and plans to take, begin to satisfy this recommendation.

## **RFID Policy and Procedures Not Developed and Issued**

US-VISIT has not developed a policy to ensure that security controls are implemented to protect its systems using RFID technology. US-VISIT performed a risk assessment and Privacy Impact Assessment to address the security and privacy of travelers' personal data during the systems design process. In addition, while US-VISIT has developed procedures for issuing and destroying RFID-enabled Form I-94s, at the time of our POE visits the procedures were not being followed consistently.

Although DHS has not developed a specific RFID policy, US-VISIT should develop its own policy. The policy should address the risks associated with the use of RFID and to ensure that adequate and effective controls are implemented to protect the integrity of data stored and

---

processed by the RFID system. For example, other federal agencies and the private sector have identified security vulnerabilities and issued notices related to the use of RFID technology, such as counterfeiting or cloning,<sup>8</sup> replay,<sup>9</sup> and eavesdropping. The introduction of these vulnerabilities increase the need to develop adequate policies and procedures to mitigate risks associated with the use of RFID technology.

Issuing a sound RFID policy is the first step to ensure that security controls are developed and implemented to protect the data on systems or mitigate risks associated with the use of RFID. Without a specific RFID policy and implementation procedures that are being followed, US-VISIT cannot ensure that effective controls are put into practice at all locations using RFID. Furthermore, RFID systems operating without specific policy and implementation procedures increase the possibility that security controls protecting DHS systems can be circumvented.

### **Recommendation**

We recommend that the Director, US-VISIT, direct its CIO to:

4. Develop and implement a policy that addresses security controls over all components of an RFID system and ensure that policies and procedures are being followed at all affected POEs.

### **Management Comments and OIG Analysis**

US-VISIT partially agreed with recommendation 4. US-VISIT will assist DHS in developing the RFID policy for the department. Once it is finalized, US-VISIT plans to adhere to DHS' RFID policy. US-VISIT will assist CBP in the development and dissemination of training materials to the POEs.

We agree that the steps US-VISIT's has taken, and plans to take, begin to satisfy this recommendation. However, we maintain that due to the lack of department-wide RFID guidance, US-VISIT should develop and implement its own RFID policy that supports its mission and operations.

---

<sup>8</sup> Cloning a RFID tag occurs when an attacker produces an unauthorized copy of a legitimate tag.

<sup>9</sup> 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.

---

## AIDMS Contingency Plan

US-VISIT certified and accredited AIDMS in January 2006. However, at the time of our review, the AIDMS contingency plan had not been tested to ensure that critical operations could be restored in the event of an emergency. US-VISIT management acknowledged at the time the system was accredited that an untested contingency plan is a security weakness and that testing was scheduled to be completed in April 2006. Contingency planning is designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of an emergency, system failure, or disaster.

Office of Management and Budget Circular A-130 Appendix III requires that contingency plans be developed and tested periodically. The *Federal Information Security Management Act* (FISMA) requires that agencies' information security programs include plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency. DHS requires the contingency plans be developed and tested annually, too. Testing of contingency plans is performed to validate specific aspects of the plan, policies, procedures, systems, and facilities that will be used in the event of an emergency. Testing the plan is also a training exercise to prepare recovery personnel for plan activation, which can improve plan effectiveness and overall agency preparedness.

When a contingency plan for a critical system is not tested, even seemingly minor interruptions can result in the loss of sensitive or mission-critical data. Since AIDMS' contingency plan has not been tested, US-VISIT cannot ensure that it will be able to promptly recover essential operations if an unexpected interruption occurs.

### **Recommendation**

We recommend that the Director, US-VISIT, direct its CIO to:

5. Test the contingency plan for AIDMS, at least annually.

### **Management Comments and OIG Analysis**

US-VISIT agreed with recommendation 5. US-VISIT indicated that, after our fieldwork was completed, the AIDMS contingency plan was tested in March 2006, and it will be tested annually.

We agree that the steps that US-VISIT has taken satisfy this recommendation.

## Purpose, Scope, and Methodology

The objective of this audit was to determine whether US-VISIT has implemented effective controls to protect its mission critical data processed by its RFID systems from unauthorized access. Specifically, we determined whether: (1) US-VISIT developed adequate policies and procedures to ensure the confidentiality, integrity, and availability of data contained on its RFID system; (2) adequate physical and logical security controls are implemented on its RFID system; (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 FISMA requirements.

To accomplish our audit, we conducted fieldwork at selected POEs located at [REDACTED]. We interviewed US-VISIT personnel at its Headquarters and CBP personnel at selected POEs. In addition, we reviewed and evaluated applicable DHS and US-VISIT 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 databases servers. Also, we used two RFID tools (spectrum analyzer, card reader) to attempt to gain information about the RFID usage at the POEs. Upon completion of the assessments, we provided US-VISIT the technical reports detailing the specific vulnerabilities detected on their databases and the actions needed for remediation.

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 G.

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.



Appendix B  
Management Response To Draft Report

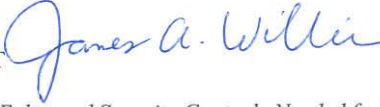
U.S. Department of Homeland Security  
Washington, DC 20528



Homeland  
Security

May 9, 2006

MEMORANDUM FOR: RICHARD L. SKINNER  
INSPECTOR GENERAL

THROUGH: James A. Williams   
Director, US-VISIT

SUBJECT: OIG Draft Report: *Enhanced Security Controls Needed for US-VISIT's System Using RFID Technology*

Thank you for the opportunity to review and provide comments on the above draft report. I was very pleased to see the determination by your office that US-VISIT has implemented effective physical security controls over the radio frequency identification (RFID) tags, readers, computer equipment, and database supporting the RFID system. I also appreciate the finding that information security controls have been implemented to provide an effective level of security on the Automated Identification Management System (AIDMS). US-VISIT's security team works diligently to minimize risk and provide adequate security controls. It is reassuring that auditors from the Office of the Inspector General came to the same conclusion.

I offer the following constructive comments for your consideration.

As more than one component within DHS is using RFID, requiring individual components—such as US-VISIT—to formulate its own policies could result in conflicting or different requirements, and could possibly prevent the interoperability of Departmental information technology systems. In addition, as noted OIG-06-016, "*US-VISIT System Security Management Needs Strengthening*," US-VISIT does not have the oversight authority necessary to direct field personnel to use or adhere to US-VISIT policies. Field personnel are mostly Customs and Border Protection (CBP) or Immigration and Customs Enforcement (ICE) agents, and they do not directly report to the US-VISIT program office. Though US-VISIT should not be the responsible entity for developing RFID policy, members of the US-VISIT program are highly involved in many DHS working groups, placing US-VISIT in an excellent position to assist in its formulation.

I regret to say that this draft report does not acknowledge the significant amount of work performed to identify potential risks of using RFID in this proof of concept system. US-VISIT specifically addressed privacy concerns in the Privacy Impact Assessment and a separate white paper, "*Radio*

[www.dhs.gov](http://www.dhs.gov)

Appendix B  
Management Response To Draft Report

Richard L. Skinner  
May 9, 2006  
Page 2 of 4

*Frequency Identification Feasibility Study*,” that examined the likelihood and potential impact of counterfeiting, cloning, replay, eavesdropping, and other issues.

It should also be noted that US-VISIT worked collaboratively with CBP and distributed Standard Operating Procedures to the five ports of entry (POEs) using the RFID technology. The Standard Operating Procedures were disseminated through the CBP Office of Field Operations (OFO). CBP OFO is the responsible entity for ensuring compliance with the official procedures. US-VISIT has no operational authority over the field offices.

The report includes the statement that “...additional controls should be implemented if US-VISIT decides, in the future, to store travelers’ personal information on RFID-enabled forms or migrates to universally readable Generation 2 (Gen2) products.” While US-VISIT is in complete agreement with the first part of the statement, the next part is misleading. If US-VISIT decides in the future to store personal identifying information (PII) on an RFID chip, additional security controls will be implemented. However, even if US-VISIT migrates to Gen2 technology, but continues to store only a number on the chip, additional security controls may not be needed. Unnecessary security controls can lead to cost overruns, performance issues, and operational constraints. To ensure that US-VISIT continues to adequately protect its systems and information, any change in the way RFID is used within US-VISIT will result in additional privacy and security risk assessments and evaluation of the appropriate controls.

I would also like to point out some specific inaccuracies in the report.

On page 4, third paragraph, the report notes that RFID technology introduces new security risks. While this may in fact be true, the vulnerability of data stored in the system database is not a new risk, and it is mitigated by controls identified in DHS policy. Indeed, without “effective security controls,” the data in any system is vulnerable.

On page 9 the report states that “...since AIDMS’s contingency plan has not been tested, US-VISIT cannot ensure that it will be able to promptly recover essential operations if an unexpected interruption occurs.” The contingency plan was tested in March 2006. As the use of RFID occurs in a proof of concept, the system is not considered “essential operations” since that would mean it is in a fully operationally environment. The loss of functionality of the RFID proof of concept would not impact operations; the processing of travelers would automatically revert to current methods.

In regard to the report’s recommendations:

*Recommendation No. 1: Develop and implement procedures to strengthen user account and password management processes relating to the AIDMS database. Procedures should include periodic vulnerability assessments and reviews of all user access.*

US-VISIT concurs with the recommendation and has already implemented procedures to strengthen account management. As the AIDMS system is operating with an Authority to Operate, it is in full compliance with the Federal Information Security Management Act (FISMA) requirements and National Institute of Standards and Technology (NIST) guidance, which require periodic

Appendix B  
Management Response To Draft Report

Richard L. Skinner  
May 9, 2006  
Page 3 of 4

vulnerability scans. Additional vulnerability scans are planned. However, because the use of RFID occurs as a proof of concept, some procedures and reviews may be deferred until the evaluation of the system is completed.

*Recommendation No. 2: Ensure that all vulnerabilities identified for which risks have not been assumed be remedied.*

US-VISIT concurs with this recommendation. All vulnerabilities identified for which risks have not been assumed have either been mitigated since the time of the audit or are being tracked for completion in the AIDMS Plan of Action and Milestones (POA&M) in the DHS Trusted Agent FISMA (TAF) tool.

*Recommendation No. 3:* [REDACTED]

US-VISIT concurs, has entered this vulnerability in the TAF, and [REDACTED]

*Recommendation No. 4: Develop and implement a policy that addresses security controls over all components of an RFID system and ensure that policies and procedures are being followed at all affected POEs.*

US-VISIT partially concurs with the recommendation. Existing security policies cover the security of information, whether it is collected through RFID or any other technical means. US-VISIT has further assessed the specific use of RFID through the Privacy Impact Assessment and an RFID Feasibility Study developed during the design of the AIDMS system. US-VISIT believes that the proper authority for developing RFID policy is DHS headquarters, and we are ready to assist in the development of that policy. Since this draft report was issued, the DHS Wireless Management Office (WMO) has developed a Draft IT Security Program Handbook for Sensitive Wireless Systems, Version 3.1, dated February 27, 2006. Additionally, the DHS WMO issued a draft Applications Implementation Guide for RFID, version 1.4, dated March 30, 2006. US-VISIT is currently reviewing these documents and will provide comments to DHS based upon our experience. Once final, US-VISIT will adhere to DHS WMO policy and guidance documents.

US-VISIT notes that the implementation of procedures at affected POEs is the purview of CBP. US-VISIT will assist in the development and dissemination of training materials.

*Recommendation No 5: Test the contingency plan for AIDMS, at least annually.*

US-VISIT concurs with this recommendation and notes that it is an existing requirement levied by DHS security policy. The AIDMS Contingency Plan was tested on March 15, 2006, and a validated artifact was uploaded into the TAF tool, POA&M tab, on the same day and in the Certification and Accreditation (C&A) tracking tab on March 29, 2006. Further testing will depend upon the continued operation of the proof of concept system. However, contingency plans for it or its successor system will be tested annually per DHS information technology security policy.

Appendix B  
Management Response To Draft Report

---

Richard L. Skinner  
May 9, 2006  
Page 4 of 4

Please let me know if you have any questions. Your staff may contact Tom Harner, US-VISIT's audit liaison, at (202) 298-5206 for further information.

Appendix C  
Types of RFID Tags and Common RFID Operating Frequencies

<b>Typical Characteristics of RFID Tags</b>			
<b>Types of Tags</b>	<b>Power Supply</b>	<b>Read Range</b>	<b>Type of Memory</b>
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

<b>Common RFID Operating Frequencies for Passive Tags</b>			
<b>Frequency</b>		<b>Typical read range and rate</b>	<b>Examples of use</b>
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.

Appendix D  
Photographs of US-VISIT Entry and Exit Lanes

---

Picture 1 – US-VISIT Entry Lane, -----



Picture 2 – US-VISIT Exit Lane -----



Appendix E  
Example of an RFID-enabled Form I-94

---

-----

**Warning** - A nonimmigrant who accepts unauthorized employment is subject to deportation.

**Important** - Retain this permit in your possession; *you must surrender it when you leave the U.S.* Failure to do so may delay your entry into the U.S. in the future. You are authorized to stay in the U.S. only until the date written on this form. To remain past this date, without permission from Department of Homeland Security authorities, is a violation of the law.

**Surrender this permit when you leave the U.S.:**

- By sea or air, to the transportation line;
- Across the Canadian border, to a Canadian Official;
- Across the Mexican border, to a U.S. Official.

Students planning to reenter the U.S. within 30 days to return to the same school, see "Arrival-Departure" of Form I-20 **prior to surrendering this permit.**

**Record of Changes**

---

---

---

**Port:** **Departure Record**

**Date:**

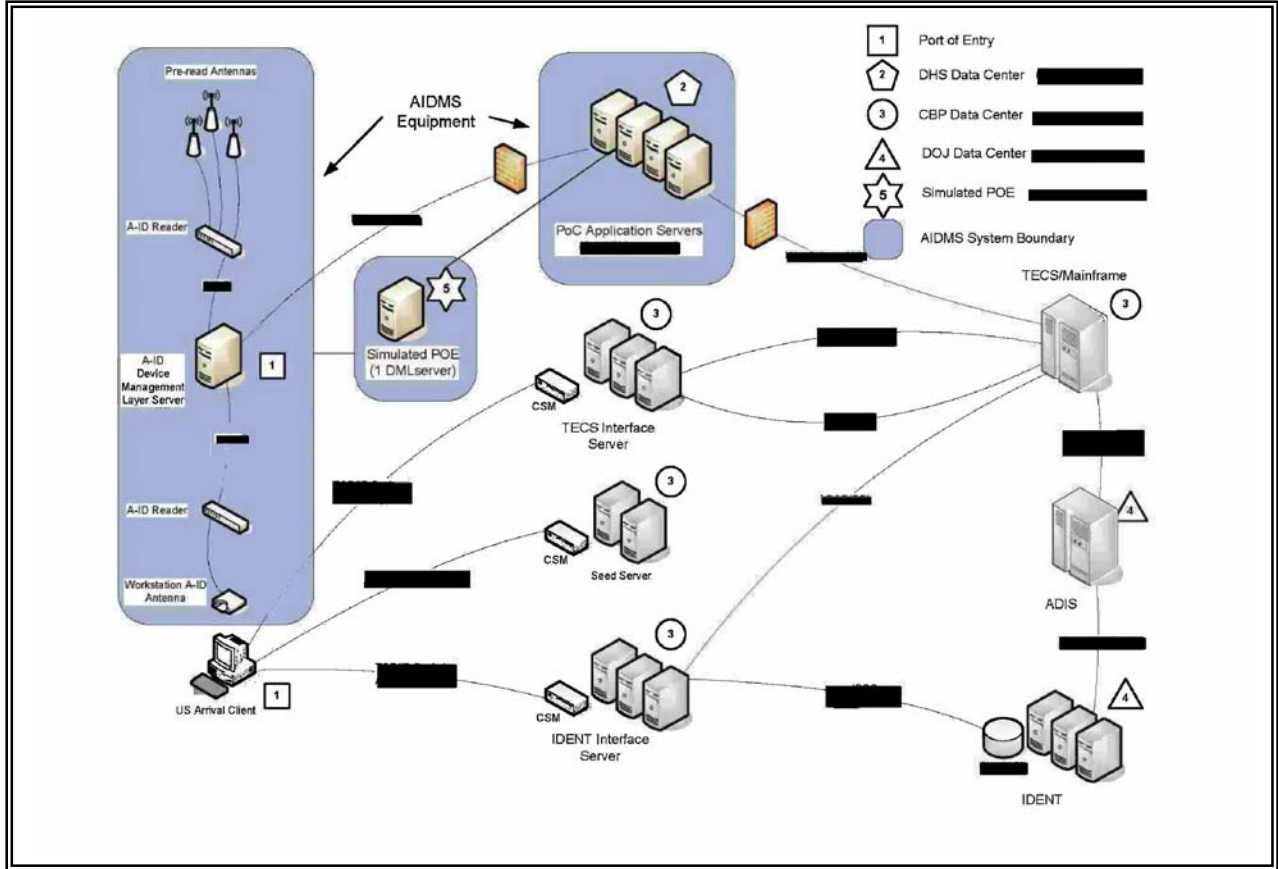
**Carrier:**

**Flight # / Ship Name:**

---

-----

Appendix F  
AIDMS Topology





**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  
Steven Staats, 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  
Assistant Secretary, Legislative and Intergovernmental Affairs  
Assistant Secretary, Policy  
Assistant Secretary, Public Affairs  
US-VISIT, Program Director  
US-VISIT, Chief Information Officer  
US-VISIT, Audit Liaison  
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](http://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](mailto:DHSOIGHOTLINE@dhs.gov). The OIG seeks to protect the identity of each writer and caller.