DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security (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-06-36 **May 2006**

Office of Inspector General

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

Homeland Security

May 31, 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 U.S. Customs and Border Protection (CBP). 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

CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
DAA	Designated Accrediting Authority
DCL	Dedicated Commuter Lane
DHS	Department of Homeland Security

Table of Contents/Abbreviations

FAST	Free and Secure Trade
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
Gen2	Generation 2
GES	Global Enrollment System
ISA	Interconnection Security Agreement
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POE	Port of Entry
RFID	Radio Frequency Identification
SENTRI	Secure Electronic Network for the Travelers' Rapid Inspection

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 tags and readers on the front end and applications and databases 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 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 U.S. Customs and Border Protection (CBP) has implemented effective controls to protect critical data processed by its trusted traveler systems. To address our objective we: (1) interviewed personnel at CBP's National Data Center; (2) reviewed applicable DHS and CBP policies and procedures; (3) conducted vulnerability assessments of the databases that collect and process information; and (4) evaluated the effectiveness of physical security and assessed the security controls over the RFID readers and RFID-enabled cards and transponders at selected ports of entry (POEs) in Detroit, MI; Blaine, WA; El Paso, TX; and Nogales, AZ.

CBP has implemented effective physical security controls over the RFID tags, readers, computer equipment, and databases supporting the RFID systems at the POEs visited. No personal information is stored on the tags used for CBP. Traveler's personal information is maintained in and can be obtained only with access to the system's database. Additional security controls would be required if CBP decides to store travelers' personal information on RFID tags or migrates to universally readable Generation 2 (Gen2) products.

However, CBP has not developed adequate policies and procedures to ensure that security controls are implemented consistently by all POEs to protect its trusted traveler systems. In addition, CBP has not implemented the necessary controls on the system's back end to ensure that the data

captured and stored for the trusted traveler programs are properly protected.

In addition, we determined that CBP did not ensure that its trusted traveler systems fully comply with all *Federal Information Security Management Act* (FISMA) requirements. For example, the systems reviewed did not have a valid authority to operate, interconnection security and user agreements were not reviewed annually, and security reviews of contractor facilities were not performed.

For the systems utilizing RFID technology, we are recommending that the CBP Commissioner direct its Chief Information Officer (CIO) to:

- Develop and implement procedures to strengthen user account and password management processes relating to the trusted traveler systems. 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.
- Develop and implement policy and procedures that address security controls over all components of an RFID system.
- Ensure that audit trails are reviewed, documented, and maintained on a regular basis.
- Ensure that all FISMA requirements are implemented, including certification and accreditation.

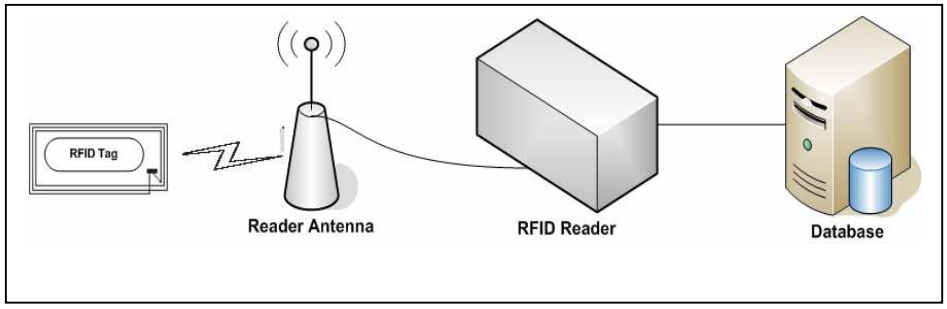
Fieldwork was conducted from November 2005 through February 2006 at selected locations. See Appendix A for our purpose, scope, and methodology.

In response to our draft report, CBP concurred with our recommendations and is in the process of implementing corrective measures. CBP'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 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 various manufacturers' RFID products and systems and different frequencies used in different countries worldwide. Gen2 features 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.[1] Among the privacy issues is notifying individuals of the existence or use of the technology.

CBP deploys RFID technology on its "trusted traveler" programs at designated border POEs to expedite the processing of pre-approved, international, and low-risk commercial and commuter travelers crossing the borders.[2] The commercial program is called Free and Secure Trade (FAST) and is propagated on the northern and southern borders. The commuter program is known as the Secure Electronic Network for the Travelers' Rapid Inspection (SENTRI) on the southern border and "NEXUS" on the northern border.[3]

SENTRI/NEXUS

The use of RFID technology was introduced into SENTRI in November 1995 and NEXUS in June 2002. As of January 2006, approximately 88,000 travelers were enrolled in SENTRI and 81,000 travelers were enrolled in NEXUS.

[1] *Radio Frequency Identification Technology in the Federal Government* (GAO-05-551, May 2005).
[2] Use of the term "trusted traveler" program(s) in this document is meant to encompass and include all programs designated by DHS and/or CBP as either "registered traveler" or "trusted traveler" programs. "Trusted traveler" and "registered traveler" programs typically require the same or similar types of personnel information to be submitted by an individual; the difference between the types of programs is the greater level of vetting and screening performed upon participants in "trusted traveler" programs.
[3] Appendix D contains photographs of a SENTRI, NEXUS, and FAST lane.

There are two systems that support the SENTRI/NEXUS program:

(1) Dedicated Commuter Lane (DCL) - is the toll lane configuration deployed at the POEs to read the RFID transponders and cards that are issued to travelers and vehicles registered in SENTRI/NEXUS. DCL consists of RFID readers, antennas, laser sensors, and video cameras. See Appendix E for depiction of DCL lane components for SENTRI/NEXUS.

(2) Global Enrollment System (GES) - is a web-based system used to collect information for travelers and vehicles that are registered in SENTRI/NEXUS. Applicants' data (for example, biographic data, photo of traveler, results of background check) is stored in a GES database. At the time of our fieldwork, CBP had incorporated all local POE databases into a centralized database except for one POE at Champlain, New York.

Currently CBP deploys Generation 1 "passive" RFID tags and Ultra High Frequency readers. Identification cards embedded with RFID tags are issued to frequent travelers who are enrolled in SENTRI/NEXUS. Within SENTRI, transponders are issued to travelers and drivers to place on their vehicles. The tags contain only a unique number, which is associated with the traveler or vehicle information that is stored in the system database. CBP is in the initial stages of identifying the resources required to migrate to Gen2 technology for its SENTRI/NEXUS program but they have not established a timeframe yet.

FAST

The FAST program became operational in December 2002. As of November 2005, there were a total of 97 lanes that were equipped with RFID readers installed at 19 border ports; 65,000 drivers have been approved; and 50,000 trucks have been registered in the FAST program. Applicants' data (for example, biographic data, driver's license, passport number, criminal record) is stored in a FAST database.

Currently, CBP deploys Generation 1 "passive" RFID tags and Ultra High Frequency readers. Identification cards embedded with RFID tags are issued to frequent drivers who are enrolled in FAST. Transponders are issued to drivers to place on their vehicles. The tags contain only a unique number, which is associated with the driver or vehicle information that is stored in the system database. CBP has no plans to migrate FAST to Gen2.

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. 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. The CBP Information Systems Security Policies and Procedures Handbook HB1400-05B aligns with the DHS Policy and Handbook and provides direction to CBP information technology users.

Results of Audit

Enhanced Security Controls are Needed to Limit Unauthorized Access to RFID Systems

CBP has not implemented effective security controls over all components of its RFID systems. To assess the security of CBP's RFID systems, we interviewed information technology personnel at its National Data Center; performed vulnerability assessments on the GES; reviewed access privileges to the GES application; evaluated physical security over RFID tags, readers, and computer equipment at the sites visited; and tested for wireless signals at selected POEs in Detroit, MI; Blaine, WA; Nogales, AZ; and El Paso, TX. Also, we reviewed the Top Secret Security software configuration settings, which are used to control access to the database, for the FAST database on the mainframe computer, in addition to the database schema and mainframe security logs and configuration files. The following table depicts the systems for each of the POEs visited during our audit.

Port of Entry	SENTRI	NEXUS	FAST
DeConcini (Arizona)	X		X
Winsor Tunnel (Michigan)		X	
Ambassador Bridge (Michigan)		X	X
Port Huron (Michigan)		X	X
Bridge of the Americas (Texas)			X
Port Zaragosa (Texas)	X		
Pacific Highway (Washington)		X	X

CBP ensured that effective physical controls were implemented over the RFID tags, readers, and computer equipment supporting the trusted traveler systems at the POEs visited. We used two easily obtainable RFID readers to assess whether unauthorized users could obtain information stored on the tags.[4] We were unable to communicate or read the information stored on the SENTRI/NEXUS and FAST cards and transponders. Furthermore, we performed additional testing in a laboratory environment with a more sophisticated reader but we were unable to read or obtain any information from the RFID tag.[5]

While data on the RFID tags is not encrypted and could be subject to interception with sophisticated RFID readers, the tags contain no personal information. To obtain personal information, data on the tag must be combined with sensitive information stored on the databases that support the trusted traveler programs. In the future, additional controls should be implemented if CBP decides to store travelers' personal information on the SENTRI/NEXUS and FAST cards and transponders or migrate to universally readable Gen2 products.

Our assessments of the GES application, centralized GES database, the remaining local GES database at Champlain, New York, and FAST database identified several weaknesses in user administration, access controls, and auditing. These weaknesses may be exploited by a user to gain unauthorized and undetected access to sensitive data. Lacking procedures to ensure that all vulnerabilities and weaknesses are identified and reviewed, management cannot ensure that the data in its critical systems is secure.

User Account and Password Management Weaknesses

CBP had ineffective user account and password management over its systems using RFID technology. While DHS has developed guidelines to implement strong passwords to restrict access to sensitive data, the results of our review indicate that these guidelines have not been implemented. In addition, the controls that have been implemented are ineffective, as CBP had established weak, inappropriate, and inconsistent password configurations over its GES and FAST databases.

4 [redacted]

5 [redacted]

SENTRI/NEXUS

During our review of the GES databases, we identified the following vulnerabilities:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

In addition, our review of GES authorized users identified ten users from the El Paso POE who used their social security number as a user ID. CBP stated that these user IDs were established when the system was being tested at the POE and were never changed when the system went into production. Since social security numbers are highly sensitive, CBP should not use social security number as users IDs; this information is captured in audit trail reports and other security documents. Improper access to and disclosure of users' social security number could lead to fraudulent activities or privacy violations.

FAST

Our review of account policy settings determined that CBP had weak, inappropriate, or inconsistent password configurations that may not be effective to protect sensitive data stored on the FAST database:

- [redacted]
- [redacted]
- [redacted]

Periodic reviews of security settings by administrators would identify security weaknesses in user and password management. Weaknesses in user accounts and passwords may result in inappropriate access to CBP sensitive data. 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.

Access Privileges Were Not Appropriately Restricted

CBP does not ensure that access to travelers' personal data is limited only to those users requiring the access in order to perform their job functions. For instance, seven Headquarter users, in managerial positions, were granted access privileges to update individual applicants' personal information, capture applicants' biometric data, and issue and disable RFID cards in the SENTRI/NEXUS system - even though their job duties do not require such access. These access privileges should be limited to personnel at GES enrollment centers where RFID cards and transponders are issued.[6]

Additionally, we determined that 22 CBP database administrators were given access to the FAST DB2 database system even though all are not responsible for database maintenance. At the time DB2 was installed, CBP management decided to grant all database administrators access to all DB2 systems, including FAST.

In addition, CBP could locate access authorization requests for only four of the 22 database administrators. CBP informed us that the majority of the users were established over 10 years ago and it is their policy to retain user access requests for three years. The documentation supplied for the four users was either an email requesting database administration access, or the document had no indication that it was reviewed or approved by senior managers, security managers, or system owners.

DHS policy requires that access control follow the principles of least privilege and separation of duties. Principles of least privilege require that each user in a system be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks. The

[6] The GES enrollment center interviews the travelers when the traveler is found eligible. During the interview, a photograph and fingerprints of the applicant are taken. Applicant's personal and biometric data are then submitted to query against other law enforcement databases for background checks or prior criminal records. If the traveler is approved for the SENTRI/NEXUS program, a RFID card is issued to the traveler and a transponder/windshield sticker will be issued to the vehicle, when applicable.

application of this principle limits the damage that can result from an accident, error, or unauthorized use.

Access authorizations should be documented on standard forms, maintained on file, approved by senior managers, and securely transferred to security managers. All active approved authorizations should be maintained on file. System owners should periodically review access authorizations listing and determine whether user access authorizations are appropriate.

Recommendations

We recommend that the Commissioner, CBP, direct its CIO to:

1. Develop and implement procedures to strengthen user account and password management processes relating to the GES and FAST systems. Procedures should include periodic vulnerability assessments, review of configuration settings, and reviews of all user access and user access forms.

2. Ensure that all vulnerabilities identified for which risks have not been assumed be remedied.

Management Comments and OIG Analysis

CBP agreed with recommendation 1. CBP has made many changes to strengthen user accounts and password management processes. In addition, CBP is in the process of updating mainframe security and operating system software to support additional password complexity management. CBP is working to develop a process to periodically review access controls and anticipates that all users will be validated beginning September 25, 2006. CBP plans to implement this recommendation fully by October 1, 2006.

We agree that the steps that CBP has taken, and plans to take, begin to satisfy this recommendation. However, CBP did not specifically address whether it will perform periodic vulnerability assessments on its databases and review user access forms.

CBP agreed with recommendation 2. CBP has initiated a requirement to track, on a monthly basis, all Plan of Action and Milestones developed to remedy vulnerabilities and risks. CBP plans to implement this recommendation by October 1, 2006.

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

Improved Policy and Procedures Need to be Developed and Distributed

CBP has not developed adequate policy or procedures to ensure that security controls are implemented to protect its systems using RFID technology. CBP personnel indicated that its current wireless policy is sufficient and there was no need to address RFID technology. While CBP has developed a wireless policy that addresses other wireless technologies, such as 802.1x, Bluetooth and Blackberry, we determined that CBP's wireless policy is incomplete, as it does not address the controls needed to protect the data stored and processed by systems using RFID technology. For example, CBP's wireless policy does not specify the controls needed to mitigate vulnerabilities that are susceptible to RFID technology, such as counterfeiting or cloning,[7] replay,[8] 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.

Operating procedures were developed to implement SENTRI/ NEXUS and FAST programs at the POEs. However, they do not address all aspects of RFID technology, such as the physical security of unused RFID cards and proper destruction of damaged RFID cards. Furthermore, CBP has not developed detailed recovery procedures for POE staff to resume operation in the event of SENTRI/ NEXUS or FAST system disruptions. Some of the POEs have developed their own procedures in lieu of guidance from CBP headquarters.

Issuing a sound RFID policy is the first step to ensuring adequate controls are developed and implemented to protect CBP's systems employing the technology or mitigating the risks associated with the use of RFID. Furthermore, RFID systems operating without required security

[7] Cloning an RFID tag occurs when an attacker produces an unauthorized copy of a legitimate tag.
[8] 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.

management practices increase the possibility that security controls protecting DHS systems can be circumvented.

Recommendation

We recommend that the Commissioner, CBP, direct its CIO to:

3. Develop and implement policy and procedures that address security controls over all components of an RFID system; and ensure that policies and procedures are distributed to all affected POEs and personnel.

Management Comments and OIG Analysis

CBP agreed with recommendation 3. CBP will draft an Interim Policy Letter to address policy and procedures for security controls over all components of an RFID system. Once it becomes a permanent policy, it will be incorporated into CBP's Information Systems Security Policies and Procedures Handbook. CBP plans to implement this recommendation by July 15, 2006.

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

Audit Trails Need to be Reviewed Regularly

CBP does not ensure that audit trails are regularly reviewed or maintained to detect modification or unauthorized access to the GES database. While user activities are captured in a GES application audit trail report, CBP has ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- . Furthermore, CBP administrators did not consistently use application audit trails to monitor user activities and there was no documentation to support that audit trails were reviewed regularly.

CBP personnel indicated that the GES application audit trail reports sufficiently captured modification access for all users and there was no need to enable the logging capability on the database. Furthermore, the contractor responsible for reviewing the audit trail reports was not provided with CBP's procedures to ensure audit trail reports are reviewed regularly.

DHS policy requires that audit trails be reviewed at least once a week. Audit trails can track the identity of each user as well as the time and date of access and log off. In addition, audit trails can capture all activities performed during a session and can specifically identify those activities that have the potential to modify, bypass, or negate the system's security safeguards.

Without prompt and appropriate reviews 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 CBP may not detect unauthorized activity or determine the users who are responsible.

Recommendation

We recommend that the Commissioner, CBP, direct its CIO to:

4. Determine the events that should be recorded in the audit trails; and ensure that audit trails for all systems are reviewed on a regular basis and maintained.

Management Comments and OIG Analysis

CBP agreed with recommendation 4. CBP will create a process directing the Information Systems Security Officers to review, document, and maintain audit trails. CBP plans to implement this recommendation by October 31, 2006.

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

Inadequate Implementation of FISMA Requirements On RFID Systems

CBP does not ensure that all FISMA requirements are met on its systems using RFID technology. Specifically, FISMA requires that each agency develop, document, and implement an agency-wide information security program. The security program should provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Agencies are required to produce a privacy impact assessment (PIA) when developing an information technology

project or when redesigning a business process that incorporates new technology. Implementing the security practices required in FISMA can help strengthen the security of RFID systems.

Certification and Accreditation

We determined that CBP's RFID systems were not properly certified and accredited. The interim authority to operate for SENTRI/NEXUS expired in February 2005. The methodology used to certify and accredit FAST was inconsistent with applicable Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and DHS guidance. For example,

- FAST was included in the certification and accreditation for many applications and servers at CBP headquarters. However, there was no mention of the FAST system in the system security plan.
- CBP did not re-certify and accredit FAST after it was migrated from an Oracle database on a Sun Solaris to a DB2 database on a mainframe computer.

CBP personnel informed us that they were in the process of certifying and accrediting DCL, GES, and FAST and expected to have all three systems certified and accredited by September 2006.

Privacy

CBP has not informed all travelers about the use of RFID technology in CBP's trusted travelers program and the possibility that applicants' data may be shared with other agencies. CBP completed the GES PIA in December 2005 and plans to use the PIA to address privacy related issues for SENTRI/NEXUS and FAST. However, the GES PIA has not been approved by the Secretary and published in the Federal Register. Our review of the GES PIA determined that it does not specifically mention each of the agencies with which CBP shares FAST data. Furthermore, we determined that not all SENTRI/NEXUS and FAST travelers are notified of the use of RFID either in writing or verbally. Last, there is an inconsistent approach to informing individuals at the POEs about the use of RFID - some POEs informed individuals in writing or verbally while others did not.

The widespread adoption of the RFID technology in the federal government can raise privacy concerns from citizens. A GAO report raised several privacy concerns related to the use of RFID technology to

track the movement of individuals traveling within the United States.[9] Specifically, the GAO report identified issues associated with RFID implementation including notifying individuals about the existence or use of the RFID technology; tracking an individual's movements; profiling an individual's habits; and allowing for secondary uses of information.

Review of Security Controls Over Contractors and Interconnected Systems Is Needed

CBP has not performed annual security reviews at all contractor facilities that support the trusted traveler program to evaluate whether adequate controls have been implemented to protect the data processed. Specifically, Mellon Bank is contracted by CBP to process all FAST RFID transponder and driver card requests from applicants along the U.S./Mexican and U.S./Canadian borders. Mellon Bank electronically transfers data between CBP and the bank. However, CBP has not performed annual security reviews to evaluate the effectiveness of controls implemented at Mellon Bank.

Also, CBP has not reviewed the effectiveness of the security controls for the interconnection between Mellon Bank and CBP since an Interconnection Security Agreement (ISA) was established in May 2004. The ISA was not signed by the FAST systems' Designated Accrediting Authority (DAA), as required by applicable NIST and DHS guidance. Our review of the ISA disclosed that the agreement has not been updated to reflect the current policies and technical environment. For example, we identified the following:

- Throughout the agreement references are made to CBP's previous security policy and procedures handbook (dated June 2001) - not the one that was issued in February 2005.
- Mellon Bank is currently deploying a different router used for encryption.

We determined that, due to management oversight, CBP has not performed security reviews at Mellon Bank. However, CBP personnel indicated that security reviews at Mellon Bank are planned for 2006.

Furthermore, our review of the user agreement between CBP and the Federal Bureau of Investigation for the sharing of applicant information in performing background checks revealed that the document does not

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

contain specific terms and conditions for sharing data and information resources in a secure manner. Specifically, the agreement does not identify the detailed responsibilities of both organizations and the timeline for terminating or reauthorizing the interconnection. In addition, there is no documentation to support that the agreement has been reviewed since it was originally signed in 1990 to ensure that the terms agreed to are still applicable and appropriate.

FISMA requires that agencies provide adequate security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor. OMB Circular A-130 requires that written management authorization be obtained prior to connecting with other systems or sharing sensitive data/information. NIST Special Publication 800-47 "*Security Guide for Interconnecting Information Technology Systems"* and DHS policy require the development of an ISA, which specifies the technical and security requirements of the interconnection, and a Memorandum of Understanding that defines the responsibilities of the participating organizations. Furthermore, each organization should ensure that its respective systems are certified and accredited in accordance with applicable guidelines before interconnecting their information systems.

Since establishing an interconnection may represent a significant change to the connected systems, each entity should recertify and reaccredit its respective system to verify that existing security controls remain effective. In addition, one or both entities should review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure the controls are operating properly and are providing appropriate levels of protection. DHS policy and NIST guidance require components to document interconnections with other networks with an ISA signed by both DAAs, and review the agreement annually to ensure that it is effective and current.

Without evaluating the effectiveness of controls implemented at its contractor facilities, CBP cannot ensure that security controls implemented are working as intended or that sensitive data processed and stored by its contractors is protected from unauthorized access and potential misuse. Security testing can lead to the discovery of potential vulnerabilities. Interconnecting information systems can expose the participating organizations to additional security risks. When one of the connected systems is compromised or not designed with adequate security controls, the interconnection could be used as a conduit to compromise the other system and the data that is stored, processed, or transmitted.

Recommendation

5. We recommend that the Commissioner, CBP, direct its CIO to:

- Certify and accredit all systems using RFID technology in accordance with OMB, NIST, and DHS guidance.
- Ensure that annual security reviews be performed at all contractor facilities.
- Ensure that all ISAs and user agreements are reviewed and updated yearly.
- Ensure that all travelers are informed of the use of RFID and that the PIA reflects all organizations that CBP shares data.

Management Comments and OIG Analysis

CBP agreed with recommendation 5. CBP will certify and accredit GES by June 2006 and the FAST system by July 2006. CBP will review all facilities when the systems they fall under are reviewed. CBP has developed a database to track ISAs and user agreements, which will be tracked monthly and updated yearly. CBP is currently providing reference guides about the use of RFID to travelers during the enrollment process and will revise and distribute a new guide by December 2006. CBP plans to implement this recommendation by December 31, 2006.

We agree that the steps that CBP has taken, and plans to take, begin to satisfy this recommendation. However, CBP did not specifically address whether it will ensure that the PIA reflects all organizations that CBP shares data.

Purpose, Scope, and Methodology

Our objective was to determine whether CBP has implemented effective controls to protect critical data processed by its RFID systems from unauthorized access. Specifically, we determined whether: (1) CBP 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 FISMA requirements.

To accomplish our audit, we conducted fieldwork at selected POEs located at: Nogales, Arizona; Detroit, Michigan; El Paso, Texas; and Blaine, Washington. We interviewed personnel at the CBP National Data Center, Mellon Bank, and at selected POEs. In addition, we reviewed and evaluated DHS and CBP 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 and card reader) to attempt to gain information about the RFID usage at the POE. Upon completion of the assessments, we provided CBP 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 F.

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 20229

U.S. Customs and
Border Protection

May 1, 2006

MEMORANDUM FOR RICHARD L. SKINNER
INSPECTOR GENERAL
DEPARTMENT OF HOMELAND SECURITY

FROM: Acting Director
Office of Policy and Planning

SUBJECT: Response to the Office of Inspector General's Draft Report on CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security

Thank you for providing us with a copy of your draft report entitled "CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security" and the opportunity to discuss the issues in this report. The U.S. Customs and Border Protection (CBP) appreciated the opportunity to work with the auditors in constructing a balanced and accurate document. CBP agrees with the overall substance and findings of the report. Identification of the issues highlighted in the report, along with the corrective measures being taken, will ensure effective controls are in place to protect critical data processed by the traveler systems using Radio Frequency Identification (RFID) technology.

The auditors acknowledge CBP has implemented effective physical security controls over the RFID tags, readers, and computer equipment supporting the RFID systems in the ports of entry (POEs). However, the draft audit report indicates CBP has not developed adequate policies and procedures to ensure that security controls are implemented consistently by all POEs to protect its trusted traveler systems. Additionally, CBP does not ensure these systems fully comply with all Federal Information Security Management Act (FISMA) requirements.

The Office of Inspector General (OIG) recommended that the Commissioner direct the Chief Information Officer (CIO) to develop and implement policy and procedures that address security controls over all components of an RFID system, and ensure that all FISMA requirements are implemented. CBP concurred with the recommendations and is taking action to address these issues.

Attached are comments specific to the recommendations. With regard to the classification of the draft report, CBP has not identified information within the report requiring restricted public access based on a designation of "For Official Use Only."

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Janiene Jones, Audit Liaison, Office of Policy and Planning, at (202) 344-2169.

Attachment

Response to Recommendations Concerning OIG Draft Report Entitled "CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security"

U.S. Customs and Border Protection Corrective Action Plan

Recommendation 1: Develop and implement procedures to strengthen user account and password management processes relating to the GES and FAST systems. Procedures should include periodic vulnerability assessments, review of configuration settings, and reviews of all user access and user access forms.

Response: CBP concurs with the recommendation. CBP has made many changes to strengthen user accounts and password management processes relating to the trusted traveler systems. [redacted] beginning September 25, 2006. CBP no longer utilizes social security numbers as user identification. CBP is working to develop a process to periodically review access control of these systems. In addition, we are in the process of updating mainframe security and operating system software to support additional password complexity management. Current user account management processes will be reviewed and additional procedures will be implemented where applicable.

Due Date: October 1, 2006

Recommendation 2: Ensure that all vulnerabilities identified for which risks have not been assumed be remedied.

Response: CBP concurs with the recommendation. CBP has initiated a requirement for tracking, on a monthly basis, all Plan of Action and Milestones developed to remedy vulnerabilities and risks.

Due Date: October 1, 2006

Recommendation 3: Develop and implement policy and procedures that address security controls over all components of an RFID system; and ensure that policies and procedures are distributed to all affected POEs and personnel.

Response: CBP concurs with the recommendation. An Interim Policy Letter (IPL) will be drafted that will address the policy and procedures for security controls over all components of an RFID system. This will encompass the GES and the Free and Secure Trade (FAST) system. Once issued, the IPL becomes permanent policy, and will be incorporated into the Information Systems Security Policies and Procedures Handbook.

Due Date: July 15, 2006

Recommendation 4: Determine the events that should be recorded in the audit trails, and ensure that audit trails for all systems are reviewed on a regular basis and maintained.

Response: CBP concurs with the recommendation. A process will be created directing the Information System Security Officers to review, document and maintain audit trails, per the direction in the draft "ISSO Guide to the DHS Information Security Program," Appendix A, page 20."

Due Date: October 31, 2006

Recommendation 5: We recommend that the Commissioner, CBP, direct its CIO to:

- Certify and accredit all systems using RFID technology in accordance with Office of Management and Budget, National Institute of Standards and Technology and Department of Homeland Security (DHS) guidance.
- Ensure that annual security reviews be performed at all contractor facilities.
- Ensure that all Interconnection Security Agreements (ISAs) and user agreements are reviewed and updated yearly.
- Ensure that all travelers are informed of the use of RFID and that the Privacy Impact Assessment (PIA) reflects all organizations that CBP shares data.

Response: CBP concurs in part with the recommendation.

- The GES will be certified and accredited by June 2006 and the FAST system by July 2006.
- Per DHS, CBP will not be performing security reviews on facilities/sites, however CBP will perform security reviews on systems. As part of the certification and accreditation process all sites will be reviewed when the system they fall under are reviewed.
- OIT has developed a database to track ISAs and user agreements, which will be updated yearly and tracked monthly.
- Currently NEXUS and SENTRI Dedicated Commuter Lane users are provided a Quick Reference Guide. Additional copies of the guide have been printed to provide to the users as part of the enrollment process. In Fall of 2006, there is a plan to harmonize the current NEXUS programs. As part of this plan the guide will be revised and distributed by December 2006. Please note that GES and FAST are two separate systems; the FAST system has its own enrollment database and should not be addressed in the GES PIA.

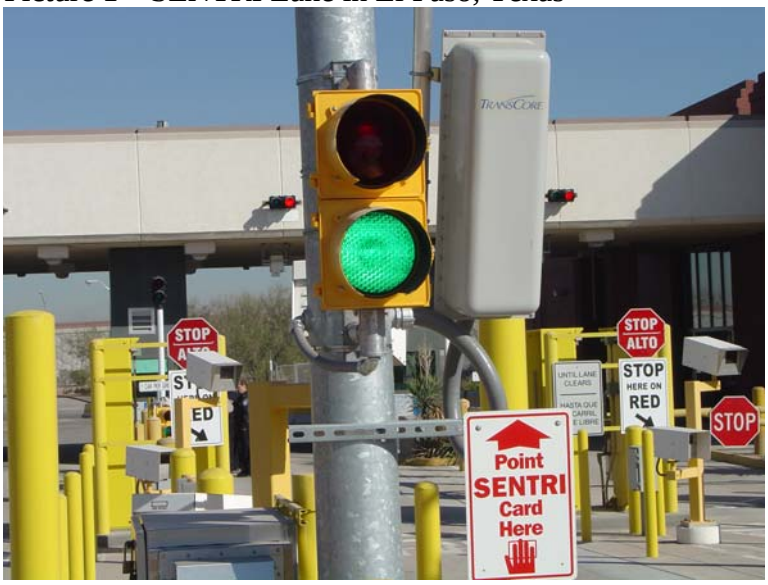
Due Date: December 31, 2006

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.

Appendix D
Photographs of SENTRI, NEXUS, and FAST Lanes

Picture 1 – SENTRI Lane in El Paso, Texas



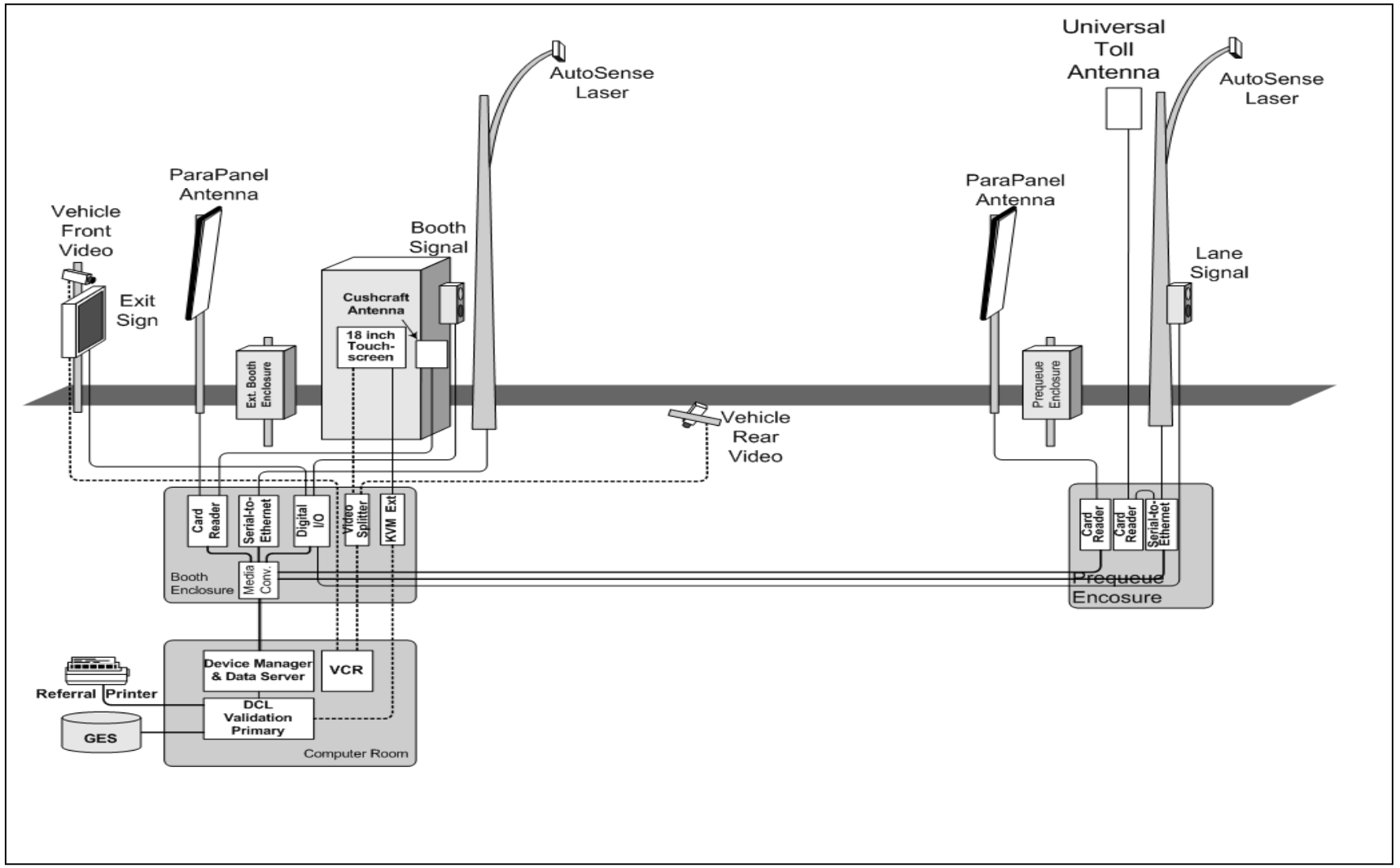
Source: Office of Inspector General

Picture 2 – NEXUS Lane in Blaine, Washington

Source: Office of Inspector General

Picture 3 – FAST Lane in El Paso, Texas

Source: Office of Inspector General


Universal
Toll
Antenna
AutoSense
Laser
AutoSense
Laser
ParaPanel
Antenna
ParaPanel
Antenna
Vehicle
Front
Video
Exit
Sign
Booth
Signal
Cushcraft
Antenna
18 inch
Touch-
screen
Lane
Signal
Ext. Booth
Enclosure
Prequeue
Enclosure
Vehicle
Rear
Video
Card
Reader
Serial-to-
Ethernet
Digital
I/O
Video
Splitter
KVM Ext
Booth
Enclosure
Media
Conv.
Card
Reader
Card
Reader
Serial-to-
Ethernet
Prequeue
Encosure
Device Manager
& Data Server
VCR
Referral Printer
DCL
Validation
Primary
GES
Computer Room

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
Karen Nelson, 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
CBP, Commissioner
CBP, Chief Information Officer
CBP, 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.

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.