DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Letter Report:

TSA's Development of Its Weapons Management System Using RFID (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-06-44 **July 2006**

Office of Inspector General

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

July 7, 2006

MEMORANDUM FOR: Edmund S. Hawley
Assistant Secretary
Transportation Security Administration

FROM: Richard L. Skinner
Inspector General

SUBJECT: TSA's Development of Its Weapons Management System Using RFID

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. The Transportation Security Administration (TSA) is developing a weapons management system using RFID in the Federal Air Marshal Service's (FAMS) Federal Flight Deck Officer (FFDO) program. While the system is in the first of three phases of development, we noted security weaknesses that should be addressed and corrected prior to the system being fully implemented.

RFID

RFID is a wireless technology that stores and retrieves data remotely. 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 controls.

Federal Flight Deck Program

The FFDO program is designed to train flight crew members in the use of deadly force with a firearm during potential terrorist hijacking efforts. Once a flight crew member has been accepted into the program, they are provided with a weapon and upon completion of training, are issued a federal identification card (credential). In conjunction with the program, the [redacted] was tasked to develop a weapons management system using RFID. RFID tags are embedded in the weapons and credentials for the purpose of providing user authentication and weapon validation. No personal data relating to the flight crew member is being stored on the tags.

The system is being developed in a three-phase approach. During Phase I, TSA is equipping weapons and credentials with RFID tags and is also creating the association in the database of the tag on the weapon to the trainee's information and credential. A handheld RFID reader and a stand-alone computer, which contains the database of trainee and weapon information, is being used at the [redacted]. This phase was completed and became operational in July 2005. Phase II will expand the number of locations (re-qualification sites) in which handheld readers will be deployed for user authentication and weapon validation and to send updated information to the database in [redacted]. In Phase III, a database server will be created on the [redacted] to replace the database in [redacted]. Since sensitive data about pilots and the weapons assigned to them are being captured in the database, it is critical that the data be properly protected.

Weaknesses in Securing the System

Based on our interviews with TSA personnel and review of applicable documentation, we noted the following:

- The system has not been included in the TSA system inventory. Even though the system is still in development, it is currently capturing operational data in support of TSA's mission, and should be accounted for in its inventory.
- The system has not been certified and accredited. FAMS management stated that the system was authorized by a TSA contractor to operate in "stand-alone" mode. According to the TSA Information Systems Security Manager, the contractor does not have the authority to authorize any system to operate. In addition, the DHS Chief Information Security Officer stated that projects in development and that use sensitive data could be certified and accredited for the duration of the project.
- [redacted]
- [redacted] Encryption is not required during this phase of development since the reader is connected directly to the computer to transfer data. However, encryption, using DHS approved encryption methodologies, should be used in future phases.

We also noted that TSA has not developed an RFID policy to ensure that security controls are implemented to protect its systems using this technology. 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.

TSA plans to migrate to a server environment in Phase II. The developers of the system plan to follow and implement all required security guidelines for federal agencies to protect data and personal information. This includes using encryption for password and data protection, and maintaining anti-virus software on the computers.

Recommendations

We recommend that the TSA Assistant Secretary direct its Chief Information Officer to:

1. Ensure that its weapons management system is included in its system inventory and an authority to operate is granted for each phase of development. All appropriate security controls, based on DHS information security procedures and configuration guides, should be implemented.
2. Develop, implement, and distribute an RFID policy that addresses security controls over all components (tags, readers, applications, databases) of an RFID system.

We hope our observations will be of assistance as you move forward in this project. Should you have any questions or concerns, please call me or your staff may contact Frank Deffer, Assistant Inspector General, Information Technology, at (202) 254-4100.

Management Comments and OIG Analysis

In response to our draft report, TSA agreed and has already taken steps to implement each of the recommendations. TSA's response is summarized and evaluated below and included, in its entirety, as Appendix A.

TSA agreed with recommendation 1. TSA and the DHS Chief Information Security Officer are conducting an inventory to determine which existing TSA system the weapons management system will become part of. TSA expects to make the determination by May 30, 2006. Further, TSA will ensure that the weapons management system is certified and accredited.

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

TSA agreed with recommendation 2. TSA is in process of developing a draft RFID policy and plans to formalize the policy before the weapons management system becomes operational.

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

****

We conducted our audit under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government audit standards.

Appendix

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

Transportation Security Administration

MAY 31 2006

INFORMATION

MEMORANDUM FOR: Richard L. Skinner
Inspector General
Department of Homeland Security

FROM: Robert D. Jamison
Deputy Assistant Secretary

SUBJECT: Transportation Security Administration's (TSA) Response Department of Homeland Security (DHS) Office of Inspector General (OIG) Draft Letter Report, OIG-06-XX "TSA's Development of Its Weapons Management System Using RFID," April 2006

Purpose

This memorandum is TSA's formal agency response to the Department of Homeland Security (DHS) Office of Inspector General Draft Letter Report "TSA's Development of Its Weapons Management System Using RFID," OIG-06-XX, April 2006. TSA thanks the DHS OIG for its work in planning, conducting, and issuing this study. The recommendations in this review will help facilitate the nationwide implementation of the Radio Frequency Identification (RFID) in the Federal Flight Deck Officer Program (FFDO).

Background

TSA developed the Federal Flight Deck Officer Program's primary weapons management system as part of its overall work flow system. TSA has implemented RFID technology to enhance sensitive item accountability and training capabilities of the program. The system is being developed in three phases. Currently, the FFDO primary weapons management tool is in Phase I and is a stand-alone database located in [redacted] Systems employing RFID technology allow any type of information to be read based on the configuration. The information that was placed on the tags used in the FFDO program excluded Sensitive Security Information (SSI) and Privacy Act information.

The distances at which RFID can be read vary, based on the type of RFID implementation selected (active, passive, or semi-active), the frequency selected, size and composition of the antenna, and the power sources available. For the purposes of this program, TSA has required the reader distance to be less than 6 inches from the RFID tag. The limited reading range and the limited information included on the tags were business decisions to ensure privacy, security, and sensitivity of the information during the research and development of the program occurring in Phases 1 and 2. Full implementation of the program is expected in 2007.

Discussion

Our plans to correct the weaknesses noted in your report are in the attached TSA response. TSA will use the findings from Phase I of the FFDO weapons management system, along with your recommendations, to improve the security and operation in the final phase of this system. The FFDO weapons management system will be implemented on a fully certified and accredited computer system.

Attachment

Transportation Security Administration's (TSA) Response
Department of Homeland Security (DHS) Office of Inspector
General (OIG) Draft Letter Report, OIG-06-XX
"TSA's Development of Its Weapons Management System
Using RFID," April 2006

Recommendation 1: Ensure that its weapons management system is included in its system inventory and an authority to operate is granted for each phase of development. All appropriate security controls, based on DHS information security procedures and configuration guides, should be implemented.

TSA Concurs: As a result of the DHS second stage review conclusion in October 2005, the Federal Flight Deck Officer Program was realigned in TSA under the management of the TSA Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS). The OLE/FAMS has begun the process of obtaining system certifications and authorities of all of TSA's law enforcement programs. OLE/FAMS expects to complete the system review by August 2006.

TSA and the DHS Chief Information Security Officer (CISO) are conducting an inventory process of the Weapons Management System (WMS) to determine if it will become part of the Judgmental Pistol Simulation System (JPS) training system or the Federal Flight Deck Officers' (FFDO) dashboard system. By May 30, 2006, TSA will determine whether it will use the WMS to track training applications or use it as a weapons inventory tool. Regardless of which system it will be used for, the WMS will follow the System Development Life Cycle methodology and ensure that the appropriate security artifacts are completed following DHS policy and the National Institute of Standards and Technology guidance. If TSA decides to use the WMS, full compliance with all Federal Information Security Management Act mandates will be obtained.

TSA's Information Security Policy is an operational element and extension of DHS's Sensitive Security Policy Directive 4300A. TSA employs a comprehensive approach to information security that requires diligence and vigilance from all managers, users, and operators. A key element of this defense-in-depth approach is the establishment, management, and enforcement of information security policy. TSA's OLE/FAMS will work through the TSA Chief Information Officer to ensure that the WMS is certified, accredited, and authorized.

Recommendation 2: Develop, implement, and distribute an RFID policy that addresses security controls over all components (tags, readers, applications, databases) of an RFID system.

TSA Concurs: The current Radio Frequency Identification (RFID) inventory program is still in the initial development stage and is not yet fully operational. TSA must develop a formal policy for implementation and application of the RFID inventory system before the program can become fully operational.

An RFID policy has been drafted and is in final stages of completion. TSA has developed IT Security and Data Integrity management directives. Also, TSA has developed security control policies at application and database levels. In addition, TSA technology specific references will be aligned with DHS policies.

OLE/FAMS is revising the FFDO program Standard Operating Procedures. This revision will include the security and control of all RFID components and information systems as recommended by DHS OIG.

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.