

**GENERAL SERVICES ADMINISTRATION
OFFICE OF INSPECTOR GENERAL**

**AUDIT OF BUILDING ACCESS THROUGH
SMART CARDS
REPORT NUMBER A040111/P/R/R05002
January 14, 2005**



U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: January 14, 2005

Reply to: Regional Inspector General For Auditing
Attn of: Real Property Audit Office (JA-R)

Subject: Audit of Building Access Through Smart Cards
Report Number A040111/P/R/R05002

To: F. Joseph Moravec
Commissioner, Public Buildings Service (P)

This report presents the results of our review of PBS's implementation of smart card technology for building access. We found that PBS's effectiveness in implementing an agency-wide credential using smart card technology has been mixed. The credentialing process needs to be better incorporated as a component of agency-wide security. A new Presidential directive on identification standards for Federal employees and contractors has impacted PBS' efforts in this area and PBS is taking action to coordinate with other agency offices responsible for security. Additionally, other aspects of the implementation, such as management controls and infrastructure, need strengthening. As such, PBS needs to: assess the smart card credential requirements and determine the estimated funding needs for GSA's smart card credentials including the costs for implementation, operations, and infrastructure; reestablish a physical security function within the PBS organization; re-evaluate and improve the management controls related to smart cards and issue additional detailed guidance as necessary; and ensure smart card credential and physical access system procurements comply with acquisition regulations and policies, including competition.

If you have any questions regarding this report, please contact me or Regina O'Brien, Regional Inspector General for Auditing, on (202) 219-0088.

for Susan P. Hall
R. Nicholas Goco
Audit Manager
Real Property Audit Office

**AUDIT OF BUILDING ACCESS THROUGH SMART CARDS
REPORT NUMBER A040111/R/P/R05002**

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
INTRODUCTION	1
Background	1
Objectives, Scope, and Methodology	3
RESULTS OF AUDIT	4
PBS has Made Progress but More Needs to be Done	4
Lack of Supporting Infrastructure	5
Inconsistent Controls	6
The Smart Card Implementation will be Impeded by Several Factors	8
Need to Integrate and Coordinate the Agency’s Security Practices	8
Interoperability Issues	9
Procurement Issues	10
The Smart Card Implementation will be Impacted by Recent Developments.	12
Conclusion	14
Recommendations	15
Management Controls	16
Management Comments	16
APPENDICES	
Management’s Response	A-1
Report Distribution	B-1

AUDIT OF BUILDING ACCESS THROUGH SMART CARDS

REPORT NUMBER A040111/R/P/R05002

EXECUTIVE SUMMARY

Purpose

The audit objective was to determine whether the Public Buildings Service (PBS) is effectively implementing a smart card credential program for security over physical access to facilities managed by the General Services Administration (GSA).

Background

Smart card technology is attractive because it can provide secure and accurate identity verification in the convenience of a small plastic card making it ideal for electronic commerce, logical access to information systems, and physical access to facilities. Within the Federal government, the objective of adopting smart card technology was to enable all employees to use one card for a wide range of purposes, including travel, small purchases, and building access. Although GSA has provided guidance and procurement vehicles for agencies to implement smart cards, until recently it had made only limited progress in implementing smart cards within the agency.

Results in Brief

PBS's effectiveness in implementing an agency-wide credential using smart card technology has been mixed. Recently, PBS established a uniform agency credential with smart card capabilities and began to issue these card credentials. However, the implementation of the smart card credentials is hindered by the lack of a vision for incorporating the smart card credential as a component of agency-wide security. As a result, the credentialing program will have only a limited impact on the security over physical access to buildings and facilities due to a variety of factors including inconsistent controls and a lack of supporting infrastructure. Further, other aspects of the smart card initiative such as integrated security practices, interoperability, and procurement issues will also be problematic for an effective implementation. Moreover, PBS's efforts will be impacted by a new Presidential directive on identification standards for Federal employees and contractors as well as the Federal Protective Service (FPS) project that will oversee smart card access to buildings and facilities.

Recommendations

We recommend that PBS coordinate with other agency officials in the development of the vision, goals, and scope for GSA's smart card implementation as part of the agency's security protocol; use the vision, goals, and scope to reassess the smart card credential requirements and determine the estimated funding needs for GSA's smart card credential including the costs for implementation, operations, and infrastructure; reestablish a physical security function within the PBS organization; re-evaluate and improve the management controls related to smart cards and issue additional detailed guidance as

necessary; and ensure smart card credential and physical access system procurements comply with acquisition regulations and policies, including competition.

Management Comments

In his January 7, 2005 response to the draft audit report (see Appendix A), the Commissioner of the Public Buildings Service (P) indicates concurrence with the report recommendations.

AUDIT OF BUILDING ACCESS THROUGH SMART CARDS

REPORT NUMBER A040111/R/P/R05002

INTRODUCTION

Background

Smart card technology is attractive because it can provide secure and accurate identity verification in the convenience of a small plastic card. A Smart Card resembles a credit card in shape and size and is embedded with an integrated circuit chip that acts as a microcontroller or computer. The chip interacts with a card reader to transact a process and provides the necessary components of system security for the exchange of data throughout almost any type of network. While smart card technology has many applications, the enhanced level of security it provides makes it ideal for electronic commerce, logical access to information systems, and physical access to facilities.

The impetus for applying smart card technology to government operations has been the past and current Administrations' push to exploit information technology, increase efficiency, streamline organizations, and eliminate barriers between organizations. The objective of adopting smart card technology was "... so that ultimately, every employee will be able to use one card for a wide range of purposes, including travel, small purchases, and building access."¹ To shepherd this transition to smart card technology, the Office of Management and Budget requested that the General Services Administration (GSA) take the lead in working with departments and agencies to develop the Federal business tools of electronic commerce and the government card services in the Federal Government in July 1996.

GSA's Role in Smart Cards

GSA has done several things to assist the adoption of smart cards. In August 1998, it established the Office of Smart Card Initiatives within the Administrator's Office to oversee the implementation of smart cards government-wide, as well as put GSA in the forefront of implementing an in-house smart card program. In addition, GSA implemented a pilot program to test Government smart cards and related systems. In July 1999, the Office of Smart Card Initiatives was transferred to the Federal Technology Service (FTS). Under FTS, GSA established the smart card business line and subsequently awarded the Smart Identification Card contract that provides Federal agencies with access to smart card services, project management, training assistance, and support. Despite this advancement as a business line, GSA's internal implementation of smart cards made little progress.

¹ The Presidential Budget for Fiscal Year 1998

On January 23, 2001, in response to an audit of GSA's internal smart cards implementation,² GSA transferred the responsibility for implementing GSA's internal smart card program from FTS to the Office of the Chief People Officer (CPO). Under this initiative, CPO established a Smart Card Working Group that included representatives from multiple organizations including CPO, the Office of the Chief Financial Officer, the Office of the Chief Information Officer, the Office of Governmentwide Policy (OGP), FTS, the Public Buildings Service (PBS), and most regions. However, this effort stalled when a fiscal year 2003 funding request of \$900,000 to implement smart cards in GSA's Central Office was not approved. Finally, on August 15, 2003, PBS was charged with developing and managing the GSA nationwide credential and building pass program based on smart card technology.

In the fall of 2003 as PBS was moving forward, a pilot project initiated by the Northeast and Caribbean Region (Region 2) implemented a smart card system in two multi-tenant buildings in New York City. Using a project team that included representatives from PBS, FTS, and the Federal Protective Service, it has issued Smart Card identification to all GSA employees as well as tenant agency personnel in the buildings and equipped the buildings with readers and barriers/portals. The smart card identifications are used alone to allow entry through the barriers/portals and in conjunction with a personal identification number and/or biometric fingerprint during heightened periods of alert.

Federal Smart Card Activities

The development of smart card technology is dynamic and the Federal government is attempting to establish uniform standards. To date, several agencies and organizations within the Federal government have been issuing guidance, policies, and specifications for smart cards. Key activities include the following:

- In August 2004, the White House issued a Homeland Security Presidential Directive³ to establish a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.
- The GSA's OGP has issued the Government Smart Card Handbook to share lessons learned and provide guidance to Federal agencies contemplating the development and deployment of smart card identity systems. This handbook was first issued in October 2000 and an update was released in February 2004.
- The National Institute of Standards and Technology (NIST) leads the development of the Government Smart Card - Interoperability Specification (GSC-IS), which establishes the technical specifications and standards for smart cards in the Federal government. The GSC-IS provides solutions to

² Review of Smart Card Initiatives, report number A000874/T/W/R00019, dated September 11, 2000.

³ HSPD-12.

- a number of the interoperability challenges associated with smart card technology. NIST issued version 2.1 of the specification in July 2003.
- In March 2004, Federal Identity Credentialing Committee (FICC) issued guidance on the use of smart card based technology in badge, identification, and credentialing systems within the Federal sector, to help agencies plan, budget, establish and implement credentialing and identification systems for Federal government employees and their agents. The document applies specifically to the use of smart card based platforms in the credentialing and identification activities of Federal government employees, contractors and affiliates supporting Federal agencies.
 - The Physical Access Interagency Interoperability Working Group (PAIIWG) within the FICC developed a standardized approach for the procurement of physical access control systems and components to ensure that agencies deploy equipment that meet both their specific needs and, at the same time, facilitate cross-agency interoperability. The guidance provides for access systems with low, medium, and high protection profiles.

Objective, Scope, and Methodology

The audit objective was to determine whether PBS is effectively implementing a smart card credential program for security over physical access to GSA facilities. We performed field work at the National Office and visited four regions: the New England Region (Region 1), the Northeast and Caribbean Region (Region 2), the Mid-Atlantic Region (Region 3), and the Great Lakes Region (Region 5).

To gain an understanding of the program, we held discussions with the PBS project team and with regional representatives involved in the implementation of the program and reviewed applicable guidance. We met with the credentialing official in the GSA Central Office, Office of Emergency Management. We reviewed the PBS task order and other procurements related to the smart card credential implementation. Additionally, we met with the FTS project manager. To gain a better understanding of smart card technology and requirements, we also met with officials in OGP as well as interagency personnel working with the Interagency Security Council, the Government Smart Card Interagency Advisory Board, and the FICC. Lastly, we spoke to officials from the Department of Homeland Security on their building security initiative.

The fieldwork was conducted between January and July 2004. The audit was performed in accordance with generally accepted government auditing standards.

AUDIT OF BUILDING ACCESS THROUGH SMART CARDS REPORT NUMBER A040111/R/P/R05002

RESULTS OF AUDIT

The Public Buildings Service's (PBS) effectiveness in implementing an agency-wide credential using smart card technology has been mixed. Recently, PBS established a uniform agency credential with smart card capabilities and began to issue these card credentials. However, the implementation of the smart card credentials is hindered by the lack of a vision for incorporating the smart card credential as a component of agency-wide security. As a result, the credentialing program will have only a limited impact on the security over physical access to buildings and facilities due to a variety of factors including inconsistent controls and a lack of supporting infrastructure. Further, other aspects of the smart card initiative such as integrated security practices, interoperability, and procurement issues will also be problematic for an effective implementation. Moreover, PBS's efforts will be impacted by a new Presidential directive on identification standards for Federal employees and contractors as well as the Federal Protective Service (FPS) project that will oversee smart card access to buildings and facilities.

PBS has Made Progress but More Needs to be Done

PBS has undertaken the responsibility for developing and implementing a nationwide standard credential system using smart card technology for the General Services Administration (GSA). PBS led the revision of the Credentials and Passes handbook⁴ to establish a standard credential for nationwide use and establish the technical specifications and topography as well as the responsibilities and accountability for the processing of the credentials. PBS also awarded a task order through the GSA Smart Card Contract for smart card identifications and their issuance. To date, PBS has ordered 18,000 cards. In January 2004, GSA began registering and enrolling employees in GSA Central Office, including the Federal Technology Service (FTS) and the Federal Supply Service (FSS), as well as in 3 additional regions⁵ through a central credentialing system database set up by the contractor. In May 2004, GSA began issuing smart cards to employees in GSA Central Office and those regions⁶. In addition, the project team has been working internally with regional personnel to prepare for the registration, enrollment, and issuance process. The project team has also been working externally with the Federal Identity Credentialing Committee and leads the Topology Working Group to develop government wide standards.

⁴ GSA Order ADM P 7640.2, dated August 15, 2003.

⁵ The New England (1), Mid-Atlantic (3), and Southeast Sunbelt (4) Regions.

⁶ As of August 4, 2004, cards had been manufactured for approximately 62% of the employees in GSA Central Office and Regions 1, 3, and 4.

According to the project team, the goal is to issue the smart card credentials to GSA employees, contractors, and tenant agency employees through a central credentialing system database. Then the cards and the database can be used to control access to GSA facilities using the smart card features. The database can be used as a control over the card through features such as an automatic expiration date and the ability to terminate a card in the database prior to the expiration date.

The card has security features for physical access such as a challenge-response system that enables a specialized reader to validate the card as well as identification information for each employee including a photograph, a fingerprint biometric, and a personal identification number (PIN). The card also includes anti-counterfeiting measures such as a hologram, ultra violet ink, and micro printing. These features improve the ability to authenticate both the card and the cardholder. What is lacking, however, is a comprehensive vision for identity management and agency security to ensure these capabilities are used optimally. To date, PBS has concentrated on issuing the credentials; but without incorporating the supporting infrastructure and stronger controls, the benefits of the smart card technology will not be achieved and the credentials, in many locations, will be relegated to a picture ID.

Lack of Supporting Infrastructure

PBS's implementation of smart cards will have only a limited impact on the physical access security of GSA facilities in the immediate future because it does not have the infrastructure to use the cards electronic security capabilities nor has it allocated funding to install the infrastructure. In adopting its card, PBS is incorporating many technology based security features such as a challenge and response card validation methodology and a centralized card termination capability, but as cards are issued, only a limited number of buildings will be able to take advantage of these capabilities in the near future. According to the PBS project team, PBS plans to equip only major Central Office locations⁷ and provide some funding to equip one building in each region with smart card access systems. As a result, few buildings will have the infrastructure necessary to actually take advantage of the smart card's security capabilities.

In addition, PBS has not allocated any funding to install additional systems in the future. Currently, the smart card implementation does not have a budget and is operating on a "pay as you go" basis using PBS National Office funds. PBS has spent approximately \$350,000⁸ to date for the credentials and their issuance, but does not have any funds allocated for the access systems or other supporting

⁷ This includes new readers for the GSA Central Office Building and a refitting of the readers at FTS locations. Readers for the FSS headquarters will not be installed until it is relocated in FY 2006.

⁸ This only includes orders placed by the PBS project team through FTS. It does not include other costs incurred by the project team such as FTS fees, travel, and salaries, nor does it include regional expenditures.

infrastructure. In addition, the project has not taken steps to estimate a budget for the supporting infrastructure. PBS has yet to inventory its buildings' current access systems or risk ratings to develop an estimate of future funds needed to implement an infrastructure for the GSA smart card credential. As such, the future costs for access systems will be the responsibility of regional management in conjunction with tenant agencies and will not be provided by PBS directly.

As a result, without a current supporting infrastructure or a funding methodology to install the supporting infrastructure, the smart card credentials will primarily be used as a picture ID at many locations. Although GSA may benefit from a uniform credential that incorporates anti-counterfeiting features and that is recognized nation-wide, it does not optimize the security capabilities of a smart card.

Inconsistent Controls

The smart card program needs consistent controls to ensure the integrity of the system and these controls must exist within the context of an agency vision of how smart card credentials will be used. The controls for the GSA smart card credential are outlined in the Responsibilities and Accountability sections of the Credentials and Passes handbook. However, the handbook provides only a broad framework for the administrative processes of issuing and terminating the credential cards. In addition, many of the policies in the handbook need strengthening as shown in the following examples:

- The smart card credential permits high-level authentication of both the card and the cardholder. However, the issuance process for smart card credentials allows for new employees to obtain a card prior to a background check. GSA's security policy does not require background checks for most new employees until after they begin working, while the credential policy calls for new employees to be entered into the credentialing database as soon as they are hired and have no requirements for the background check to be completed prior to obtaining a card. Additionally, the credential policy only requires contractors performing work requiring a moderate or high-risk clearance to have a background check or clearance. Several prior audits⁹ have identified contractor background checks as a security weakness as these clearances often are not performed or updated when required.
- Although the Credentialing Office is required to maintain an electronic system of checks and balances and controls, the credentialing system currently does not have any reporting or querying capabilities that could be used as part of a system of controls or checks and balances¹⁰. In fact,

⁹ Audit Report Numbers A030086/P/2/R04001, A020143/P/5/R03014, A81543/P/5/R99510, A995160/P/5/R00007, A001053/P/5/R01020, and A010230/P/5/R02023.

¹⁰ The task order specified that the card management system must track ID expiration, application and container management, revocation, smart card deactivation, and basic and ad hoc report

when credentialing officials were verifying individuals prior to card issuance, they could not query the system to identify personnel whose data was incomplete because the database only provides data at the individual level and cannot perform queries at a group level. For example, the system could not be queried to identify personnel who had pictures and fingerprints taken, but had not registered on-line. Moreover, to actually verify the data as correct, the registration data had to be manually verified to information from GSA's human resource database.

- According to the handbook, the GSA Office of the Chief Information Officer (CIO) has the responsibility for operating and maintaining the credential system hardware and software, as well as being the point of contact for changes to the database. However, although the GSA CIO has agreed to house the credentialing system's server in its secure space, it has not taken any more responsibility for any other aspects of the system.
- Ensuring updated employee information in the credentialing database is unreliable as it is dependent on GSA employees to submit revisions to their supervisor who submits the data to the Credentialing Office. Data updates would be more reliable if the credentialing system could be updated with data from GSA's human resource database; however, the PBS task order did not provide for the credentialing system to interact with any GSA systems.
- According to the handbook, supervisors collect the credentials from separating employees and the Office of the Chief People Officer (CPO) will return the credentials to the credentialing office. However, according to a representative from CPO, supervisors are responsible for ensuring separating employees return their credential to the credentialing office.
- The Office of Emergency Management (OEM) is charged with conducting reviews of GSA's Central Office and the National Capital Region (NCR) to ensure compliance with agency policies and guidance. However, the OEM is the credentialing office for Central Office and has a conflict of interest in reviewing its own operations. In addition, the credentialing official in OEM stated that his authority does not extend to NCR and he would work to revise the handbook.

The handbook provides only part of the guidance necessary for a successful implementation; an agency vision is needed to provide a contextual framework. We recognize that balancing GSA's and tenant agencies' security needs with public access is a complex and difficult task. What we have found though, is that key decisions such as which buildings should have card readers, whether to integrate physical barriers with the authentication process, and when the PIN and

generation. However, in a discussion, a representative of the vendor stated that if PBS needed reports, the function could be programmed into the system for a fee.

biometric features should be used are not addressed and are left to the individual regions to determine. Further, the regional Credentialing Offices are responsible for establishing agreements with tenant agencies, but there is no guidance with regard to what needs to be included in the agreement. Without reliable and consistent policies and procedures, it will be difficult to maintain a strong uniform approach to security.

The Smart Card Implementation will be Impeded by Several Factors

Other factors will also impede PBS's implementation of smart cards. These factors include the need to integrate the agency's security practices, interoperability, and procurement issues.

Need to Integrate and Coordinate the Agency's Security Practices

PBS's ability to effectively implement smart card credentials is affected by other security responsibilities within the agency that are separate and distinct from implementing the smart card credentials. To obtain the most benefit from this implementation, the agency's security practices need to be integrated and coordinated with the implementation of the smart card credential at both the functional and organizational levels. Although, in recent discussions, the Deputy Commissioner has indicated that PBS has begun coordinating on these issues with other organizations within the agency, GSA needs to address several agency-wide security functions and responsibilities that are necessary to properly implement smart cards.

For example, personnel security is vital to a smart card implementation because it establishes the identity of the smart card recipient and ensures that the recipient meets the suitability requirements to become a government employee and receive a card. However, as discussed earlier, GSA's personnel security policy and procedures, dated January 15, 1998, do not require this determination to be made for most GSA positions until an employee has already begun working. As a result, employees may become eligible for a smart card before their identities are confirmed and their security requirements are investigated.

In addition, since smart cards can enhance both physical and logical access¹¹ security, these functions should have representation on the PBS project team so that the program can incorporate their needs. However, GSA has not fully addressed these functions within the agency. With regard to physical security, FPS handled those policies and practices in the past, but that organization was transferred to the Department of Homeland Security in March 2003. To date, GSA has yet to fill this void. Within PBS, the most recent update to its organization manual provided for a subject matter expert for security, but the position has not been filled and the function is not being performed. Likewise, logical security function is not being integrated with smart cards either. The GSA

¹¹ Logical security is responsible for access to information technology such as computer networks and applications.

CIO IT Strategic Plan calls for the agency to pursue technologies such as smart cards that offer solutions to improve logical access control. However, currently, GSA is not actively pursuing the use of smart cards for logical security and the GSA CIO has not actively participated on the PBS project team.

The PBS project team also does not have a means to coordinate the smart card responsibilities of other GSA organizations as previously discussed. Although PBS is charged with managing the smart card credential and building pass, all GSA organizations are stakeholders. Not only is the smart card being issued to all GSA employees, but also many organizations will be involved in the smart card operations. According to the handbook, the CPO is responsible for notifying the Credentialing Office of separating employees, the CIO is responsible for operating the credentialing system hardware and software, the Office of the Administrator and regional management will be devoting employees to the regional credentialing office, and all service and staff offices and regional management must designate supervisors who can approve employee applications for the smart card credentials. However, these stakeholders are not members of the project team and so PBS lacks the communication channels necessary to coordinate and collaborate with the other GSA organizations in performing their responsibilities related to the smart card credentials.

Interoperability Issues

The federal government intends to adopt smart card technologies so that a card issued by one agency can be used for a wide range of purposes throughout the government. However, the GSA credential includes two features, the fingerprint biometric and the electronic challenge-response card validation, which hinder this goal. The incorporation of these features into physical access control systems will limit the ability of cards issued by other agencies to be used within GSA managed buildings and facilities.

Biometric Information: According to the Federal Identity and Credentialing Committee (FICC) smart card policy¹², each smart card should have the capability for a biometric. However, to date, the federal smart card community has not adopted biometric technical specifications and most vendors offer biometric models that are implemented using proprietary technology, which limits interoperability. Likewise, GSA's smart card uses a fingerprint biometric that is based on proprietary technology and as such, the interoperability of the GSA access systems will be limited. As there are many variations of biometrics and readers are primarily geared toward one specific version, cards issued by other agencies may not have the full capability to access GSA facilities.

Challenge-Response Card Authentication: GSA's smart cards will employ an electronic challenge-response authentication method, known as the High

¹² Policy Issuance Regarding Smart Card Systems for Identification and Credentialing of Employees issued in March 2004.

Assurance Profile¹³. This methodology is an enhanced security feature in which an encrypted algorithm stored on the card's memory interacts with a specialized reader to verify that the card is valid and issued by a legitimate government organization. The readers will reject smart cards that do not have the correct algorithm. The developer of this methodology is a subcontractor on PBS' task order. GSA is one of only a few agencies that have adopted this feature.

As a result of the adoption of these features, PBS has created a specification for GSA buildings that is not readily interoperable with smart cards issued by the majority of other agencies. In fact, GSA is already experiencing interoperability issues internally. The GSA Northeast & Caribbean Region (Region 2) began implementing a smart card system at 26 Federal Plaza in New York City prior to the PBS' initiative and used a different contractor. These cards were distributed to all Federal employees in the building - GSA employees as well as other federal tenants. These cards do not have the same biometric as the GSA card and do not have the challenge-response algorithm. As a result, the cards and the card reader equipment at 26 Federal Plaza will not be interoperable with the GSA card. Currently, the region is planning to migrate to the GSA credential and replace equipment as necessary.

In the future, these interoperability issues may be addressed as the policy for a common identification standard evolves.

Procurement Issues

The PBS smart card task order had a limited scope. It basically covered the equipment and services for the issuance of cards and the readers needed to equip one building in each region. However, it did not cover all of the equipment necessary for the issuance nor did it include all of the equipment and services to install physical access control systems. As a result, regional management has been procuring equipment and services outside of the PBS task order and this has led to problems with the ordering and pricing of data capture stations as well as competition for access systems.

Data Capture Stations: To date, several regions have been making procurements for the data collection hardware and software, known as data capture stations. The PBS task order allowed for the purchase of between 2 and 15 stations. In preparing to issue cards in the regions, PBS stated that it would be supplying each region with one station and that the regions would need to purchase additional stations on their own. To meet their needs for additional data capture stations, the regions need to conform to the same equipment provided by PBS. However, they have been acquiring the equipment from PBS' contractor

¹³ In standards for physical access controls systems published by the Government Smart Card Interagency Advisory Board (GSC-IAB), a challenge-response system is a permissible methodology for contact cards. However, the GSC-IAB has not sanctioned using the challenge-response methodology on a contact-less card as it requires proprietary technology.

and subcontractor using multiple purchasing arrangements with inconsistent pricing and terms.

PBS began purchasing data capture stations through its task order that was awarded under the GSA Smart Card Contract and required PBS to pay a fee to FTS. As the regions needed to purchase the stations, the PBS project team began recommending that the regions use Federal Supply Schedule contracts to save money. As such, Region 4 purchased a station citing a supply schedule contract for Financial and Business Solutions¹⁴ held by the prime contractor for the PBS task order and Region 1 purchased two stations citing a supply schedule contract for General Purpose Commercial Information Technology Equipment¹⁵ also held by the prime contractor. However, these supply schedule contracts do not include smart card equipment such as the data capture station and are out of scope. These acquisitions were within the dollar threshold for simplified acquisitions, which allows purchases based on a quotation without a contract in place. This methodology was essentially used by Region 3, which cited no contract with its payment.

In addition, the pricing and terms on these purchases have been inconsistent. The PBS task order price for a data capture station is \$4,667.05¹⁶, including labor, set up, support, and training and the related travel costs are to be reimbursed at actual cost. Under a price quote from the prime contractor to PBS on January 12, 2004, the regions could purchase additional enrollment stations at the same price of \$4,667.05 including labor, set up, support, and training. However, in March 2004, Region 1 purchased two stations from the prime contractor at a total cost of \$11,334 or \$5,667 per unit and Region 3 received two stations from the subcontractor for the same price. According to the subcontractor, the additional charge is for travel and labor related to setting up the machine and training employees to use the station, although labor was previously included in the base price of the station. In August 2004, the subcontractor provided PBS with a new quotation that established a standard price \$4,667 per station and \$2,000 charge for on site setup and configuration, effective through the end of fiscal year 2004. In the future, the costs for data capture stations will increase more as the subcontractor is currently in the process of adding data capture stations to its Federal Supply Schedule contract at a price of \$9,694.25.

Access Systems: The PBS task order did not include physical access control systems. However, the PBS contractor team may have a competitive advantage on these procurements due to knowledge of the GSA smart card technical characteristics and its role on the PBS task order.

¹⁴ Contract Number GS-23F-0016J.

¹⁵ Contract Number GS-35F-4338D.

¹⁶ The original negotiated price was \$3,067.05, but was increased through a modification to add a Custom Lighting Array for the equipment.

Only PBS' contractors have full knowledge of the GSA smart card's technical characteristics and as a result, the competition on the regional procurements is being affected. For instance, when Region 1 procured access and control systems for two of its buildings, there were only two bidders, the PBS prime contractor and one competitor that had lost on the PBS task order. However, this competitor initially could not submit a proposal because it lacked technical information for the GSA card's data model. Eventually, GSA had to obtain that from the PBS contractor, so the competitor could submit a bid. Also, when Region 3 was procuring an access system for its regional office building, this same competitor complained because GSA was forwarding its questions relating to the technical aspects of the GSA card to PBS's subcontractor, who was also competing on the acquisition. Eventually the competitor declined to submit a proposal.

Lastly, the subcontractor has been working closely with the PBS project team to issue the GSA credentials and with the regions in setting up the initial equipment provided by the PBS National Office. As such, the subcontractor's role on the PBS task order also creates the appearance of a competitive advantage. For example, when Region 3 initiated a procurement to replace the card readers in its regional office building to make them compatible with the new GSA smart card, it did not intend to hold a competition. The subcontractor on the PBS task order had been involved in meetings between Region 3 and the PBS project team, and after discussions with Region 3 about its future requirements, had been providing price quotes to the Region. The region had initially planned to make the procurement on a sole-source basis to the subcontractor through a Federal Supply Schedule contract. However, after receiving complaints, Region 3 held a competition. But as discussed above, the subcontractor, as GSA's technical expert, fielded its competitor's technical questions.

Since the PBS task order did not cover the full scope of GSA's needs, additional procurements for smart card equipment, systems, and services will need to be made. In making these procurements, GSA should ensure that these future procurements comply with proper procurement methods, provide consistent pricing and terms, and avoid limits on competition.

The Smart Card implementation will be impacted by recent developments.

Two recent developments, specifically the Presidential directive on common identification standards for Federal employees and contractors and the Federal Protective Service's (FPS) smart card building security program, will affect the current smart card implementation.

On August 27, 2004, a Homeland Security Presidential Directive¹⁷ was issued to provide for a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to employees and

¹⁷ HSPD-12.

contractors that will be established within six months of the directive's date. This directive has the potential for disrupting the PBS project by adding more requirements over the issuance of the credentials as well as for their implementation. For example, the Federal standard for secure and reliable forms of identification will require sound criteria for verifying an individual's identity. The requirements to obtain a GSA credential may not meet this standard because, as discussed earlier, new GSA employees and contractors may be able to obtain the GSA credential without security or background checks. As all agencies are required to have a program in place to meet the standard, GSA may be required to tighten its controls over the credentials and adjust the implementation.

In addition, FPS is planning to implement a building security program using smart cards for federal facilities. FPS plans to include a central card management system that will be linked to agencies' human resources or payroll database and that can immediately control access as cardholders enter or leave government employment. The FPS system would also link the background clearance investigations process to the issuance of government identification to employees. FPS also plans to integrate the smart cards access systems into the existing communications and dispatch networks, called Mega Centers, that currently monitor security at federal buildings and perform remote troubleshooting of perimeter building alarms 24 hours per day, 7 days per week.

GSA's credentialing program and the FPS system have similar objectives and clearly overlap in some areas. Coordination is especially needed to not only ensure compatibility with the GSA smart card implementation, but to also clarify the responsibilities of both agencies with regard to the following:

- *Who has responsibility for access to GSA properties?* According to the PBS project team, FPS is responsible for the perimeter security of GSA properties, while GSA controls who has the right to access those properties. However, this may conflict with FPS's responsibility to develop building access requirements.
- *Are smart card access systems defined as security equipment?* According to the Memorandum of Agreement regarding the transfer of FPS from GSA to the Department of Homeland Security, control and custody of the security equipment purchased and installed by GSA should be transferred to FPS and FPS will be responsible for the maintenance, repair, and replacement. In discussions, FPS personnel stated that smart card access systems are considered security equipment. Conversely, according to the PBS project team, the smart card readers are part of the card management systems.
- *Will FPS make smart card access systems mandatory security equipment?* According to the Memorandum of Agreement between FPS and GSA, GSA is responsible for funding security features and equipment on new construction and major repair and alteration projects. However, on minor repair and alterations projects, GSA only funds non-mandatory security enhancements, while FPS is responsible for funding the purchase

of mandatory security equipment. As such, if FPS makes smart card systems mandatory for more Federal properties, it may be responsible for funding these systems and relieving GSA of that burden.

Although GSA and FPS have been working together at the local level to install building access systems and have contact at high levels, PBS needs to start coordinating with FPS on plans for smart card access to federal facilities to ensure these issues are resolved.

Conclusion

While PBS has been very focused on acquiring the smart card credentials and has made progress in this area, there are significant gaps in the integration of smart card technology into the agency's security process. The agency is buying smart card technology without fully assessing what its needs are and without providing the corresponding infrastructure to support these needs. The issuance of credentials will not result in a nationwide security system if each region develops its own controls and implements its own supporting infrastructure independently of each other and organizations such as the CIO and CPO play only tangential roles.

The Government Smart Card Handbook¹⁸ recommends that, prior to acquiring smart cards, an agency assess its needs based on such areas as its security requirements, size and geographic distribution, need for interoperability and available resources in order to establish the vision, goals and scope for implementing the smart cards. It is critical that GSA understand its own specific requirements and goals for the smart card credential. While it is important to consider future requirements, it is equally important that the program not incur unneeded expense to obtain technologies that are beyond the agency's basic implementation needs.

The vision, goals, and scope for implementing the smart card credential need to be defined because it is this framework that guides all subsequent decisions about the card including the card requirements, interoperability, and funding. While the card has additional functionalities for logical access to information systems and other uses, it is currently only intended as a credential for physical access to buildings. The card has some high-level security features yet how these features fit into our overall security program or when they should be used has not been defined. Additionally, regions will be responsible for determining how the cards will be used and providing funding to support their decision. There are no assurances that the equipment necessary to activate the features or additional security controls such as physical barriers integrated with card readers that would make the features more formidable will be funded. Further, these features appear to be a major factor in the selection of the contractor, as the technology for some features is not widespread.

¹⁸ Issued by the GSA Office of Governmentwide Policy.

The implementation of GSA's smart card credentials is facing an array of issues that need to be addressed beginning at the agency level. To accomplish this, PBS needs to establish an integrated team to consider the options, scope, opportunities and impacts of the smart card program the agency develops. The team should include individuals representing the major stakeholders in the agency's smart card credentials rather than relying solely on PBS personnel. Personnel from the CIO, the CPO, FSS, FTS, and regional management are also essential for the team. Next, in order to achieve interoperability across other agencies, consideration must be given to the new requirements for a common identification, consideration also needs to be given to the impact of the FPS smart card initiative, and other work within the Federal smart card community. Moreover, arrangements or Memorandum of Understanding must be put in place if the costs of the card implementation are to be shared across agency departments, programs, or external agencies. In addition, the funding allocation formulas should be specified in interagency agreements when multiple programs or offices are to fund the card platform.

To help carry the smart card credential forward, PBS also needs to reestablish a physical security function. The physical security function could act as the champion for the smart card credential within the agency. However, its role should extend beyond issuing of the smart card credential and include coordinating the activities needed to implement comprehensive policies and procedures to enhance the overall agency security as it relates to the smart card program especially with regard to identity management and physical access. Its role could also include being the liaison with other Federal entities involved in building security, such as FPS and the Interagency Security Committee.

Smart card technology is a powerful enabling tool that can greatly improve the effectiveness and efficiency of the agency. A smart card credential can provide the basis for new levels of trust, more effective physical access to buildings, and more secure logical access to information systems with enhanced information assurance. With such systems, access to buildings and information systems can be much faster for trusted entrants, while much more effective in preventing unauthorized access. To achieve these benefits, PBS will need to provide the leadership to accomplish the vision and goals for the implementation of the smart card credentials within the agency.

Recommendations

We recommend that the Commissioner of the Public Buildings Service:

1. Coordinate with other agency officials in the development of the vision, goals, and scope for GSA's smart card implementation as part of the agency's security protocol.
 - a. Include representatives from the major stakeholders such as the CIO, CPO, and the regions.

- b. Establish an integrated project team to implement GSA's smart card credential.
2. Use the vision, goals, and scope to reassess the smart card credential requirements and determine the estimated funding needs for GSA's smart card credential including the costs for implementation, operations, and infrastructure.
 - a. Ensure the interoperability of the smart card credential and access systems by adhering to the specifications and standards set by the Federal community and avoid incorporating technology that limits interoperability.
 - b. Coordinate with FPS regarding building security decisions, smart card interoperability, and funding for the smart card infrastructure.
 - c. Establish a program to ensure compliance with the Federal standard for secure and reliable forms of identification when it is issued.
3. Reestablish a physical security function within the PBS organization.
4. Re-evaluate and improve the management controls related to smart cards and issue additional detailed guidance as necessary.
5. Ensure smart card credential and physical access system procurements comply with acquisition regulations and policies, including competition.

Management Controls

The management controls related to the smart card implementation are weak as discussed above.

Management Comments

In his January 7, 2005 response to the draft audit report (see Appendix A), the Commissioner of the Public Buildings Service (P) indicates concurrence with the report recommendations.

AUDIT OF BUILDING ACCESS THROUGH SMART CARDS
REPORT NUMBER A040111/R/P/R05002

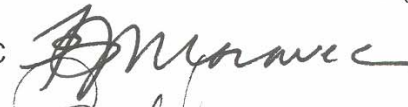
Management's Response




GSA Public Buildings Service

JAN 7 2005

MEMORANDUM FOR REGINA O'BRIEN
REGIONAL INSPECTOR GENERAL FOR AUDITING (JA-R)

FROM: F. JOSEPH MORAVEC 
COMMISSIONER (P)

THRU: ANTHONY E. COSTA 
DEPUTY COMMISSIONER (PD)

SUBJECT: Draft Report: Audit of Building Access Through Smart Cards
Report Number A040111

The Public Buildings Service appreciates the opportunity to submit comments on the subject Office of Inspector General draft audit report. Attached are our comments.

PBS believes it developed a clear vision, scope, and goals for implementing the GSA common ID cards and processing system. PBS embarked on this initiative as a pilot program in New York prior to implementing it nationwide. As you recognized in the draft audit, GSA is unique among the Federal agencies in that our buildings serve as host to tenants from many agencies. GSA has made great strides in becoming a leader in the Federal Smart Card community.

We feel we have made good progress overall in the issuance of common ID cards. The broader issue of personal identity verification, though, has become more complex as a result of Homeland Security Presidential Directive 12 (HSPD 12). This presidential directive mandates a government-wide standard for secure and reliable forms of identification. GSA is an active participant in this effort being led by the National Institute of Standards and Technology (NIST). Draft Personal Identity Verification (PIV) Standards are scheduled for development and promulgation by February 28, 2005. Standards regarding common ID cards will be part of the issuance. Because we have helped lead this initiative, we expect the draft standards will be fairly consistent with what we have implemented. At the same time, work associated with this effort has helped us refocus on some of the broader issues regarding personal identification standards and processes within GSA.

Based on our experience with the program, issuance of HSPD-12, and findings included in your draft, PBS agrees fully that more Agency and, indeed, government-wide coordination is essential for continued success of the Smart Card implementation nationwide. We have taken the following steps to improve coordination in both arenas:

1. External Government-wide Initiatives. GSA is involved with the following government-wide initiatives: the NIST, the Smart Card Interoperability Advisory Board (IAB), and the new committee established by OMB, Federal Identity Credentials Committee (FICC). On January 19, 2005, GSA, in partnership with the Department of Commerce and OMB, will hold a public meeting, which will cover policy, privacy, and security issues associated with the PIV standard for Federal employees and contractors.
2. Internal GSA Initiatives. In December, PBS hosted a meeting with GSA's Chief Information Officer, Chief People Officer, and Office of Government-wide Policy to examine the status of the program, proposed impacts relating to implementation of HSPD-12, and our current program management structure. As a result of the meeting, a new GSA-wide steering committee was established to better coordinate the program and associated business practices across the agency.
3. Joint (government-wide and GSA) Initiative. The Government Smart Card Handbook was developed under the joint sponsorship of the GSA Office of Governmentwide Policy and the Smart Card IAB (issued February 2004). This document addresses many of the findings in the IG audit.

Again, thank you for the opportunity to respond to the draft audit report. If you have any questions, please contact Mr. Anthony Costa on (202) 501-1100.

**AUDIT OF BUILDING ACCESS THROUGH SMART CARDS
REPORT NUMBER A040111/R/P/R05002**

Report Distribution

Commissioner, Public Buildings Service (P) 3

Office of the Chief Financial Officer (B) 2

Assistant Inspector General for Auditing (JA, JAO and JAS) 3

Assistant Inspector General for Investigations (JI) 1

Branch Chief, Audit Follow-up and Evaluation Branch (BECA)..... 1