IMPROVEMENTS NEEDED IN MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS FOR PBS' STAR SYSTEM REPORT NUMBER A040159/P/T/R05006

March 31, 2005

IMPROVEMENTS NEEDED IN MANAGEMENT,
OPERATIONAL, AND TECHNICAL
CONTROLS FOR PBS' STAR SYSTEM
REPORT NUMBER A040159/P/T/R05006

TABLE OF CONTENTS

PAGE

APPENDICES

IMPROVEMENTS NEEDED IN MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS FOR PBS' STAR SYSTEM
REPORT NUMBER A040159/P/T/R05006

EXECUTIVE SUMMARY

Purpose

The General Services Administration's (GSA) Public Buildings Service (PBS) is responsible for the oversight of an inventory of more than 8,900 buildings and 340 million square feet of office and warehouse space. The System for Tracking and Administering Real Property (STAR) is PBS' mission critical information technology (IT) investment managed by the Office of the PBS Chief Information Officer for providing realty specialists and portfolio managers the capability to input and update business data. PBS relies heavily on STAR as the primary tool used to track and manage the government's real property assets and to store inventory data, billing data, building data, customer data, and lease information. STAR manages aspects of real property space management, including identification of all building space and monthly billing for all property to its client Federal agencies. The objective of our review of STAR was to assess how the system is meeting management and user requirements, and the effectiveness of system security controls.

Background

For a number of years, PBS experienced problems with its real property management information systems. Functions were limited, the same data had to be input multiple times into several systems, old software was unreliable and difficult to maintain, and PBS experienced problems with data accuracy. PBS conducted extensive market research and analysis beginning March 1994 to evaluate various alternative real estate information systems. STAR was deployed in 1997 to help PBS become more effective at managing government properties and related annual rent billings. Initially, the system was primarily used by PBS realty and revenue specialists in the 11 GSA regions. STAR has since been expanded to support the security function in the Federal Protective Service mega-centers, to bill other Federal agencies for rent, to provide management information for GSA and other Federal managers, and to exchange information with other systems through the PBS Data Gateway System.

Results-in-Brief

STAR was developed to provide improved functional capabilities for many of PBS' business processes. Management, operational, and technical controls for the system, however, need to be strengthened to better provide necessary functional capabilities in support of PBS' business processes. Recent organizational, business, and system changes have challenged PBS' ability to manage STAR efficiently and effectively, and in a manner consistent with enterprise architecture goals for information technology. While PBS has taken steps to improve the collection and reporting of performance measures through the STAR business case, additional steps are needed to establish and achieve system-specific measures and goals for long-term efficiency and effectiveness. Further, PBS has not yet completed a comprehensive data dictionary for STAR that can be leveraged across the organization to effectively support business functions. System security weaknesses requiring action include the need to: (1) complete background checks for contractors supporting STAR prior to providing them with access to the system and its resources; (2) capture additional detail with audit trails to support investigations should normal system operations cease; (3) reassess whether additional protection for system interfaces is warranted; and (4) develop a more comprehensive approach to monitoring risks with the system. Taking steps to strengthen management, operational, and technical controls for STAR will better enable PBS to ensure long-term success for this mission-critical system by providing the information needed to effectively manage its real property assets.

Recommendations

In order to strengthen managerial, operational and technical controls for the STAR system, we recommend that the Commissioner, Public Buildings Service, work with the PBS-CIO to ensure that:

1. STAR provides necessary business line management information through:
   a. System enhancements, which are consistent with enterprise architecture goals.
   b. System-specific performance measures for identifying and monitoring progress with meeting established goals and system requirements.
   c. A complete system data dictionary designed to capture the comprehensive nature of information in STAR and more effectively leverage the system across the organization.

2. Adequate security controls are in place to manage risks with STAR by:
   a. Completing necessary background checks for contractor staff as required by the GSA IT Security Policy and implementing compensating controls, as necessary, until this process is completed.
   b. Enhancing the system's audit trails to provide an effective control for capturing a snapshot of information at any given time to better enable system monitoring and recovery.
   c. Reassessing the risk of not encrypting the transmission of sensitive STAR data.
   d. Updating the system risk assessment, security plan, and business continuity plan to more comprehensively address potential system threats and vulnerabilities.

Management Comments

In his March 31, 2005 response to our draft report, which is included in its entirety as Appendix A, the PBS Commissioner generally concurred with the findings and recommendations presented in our report. Written comments provided by the Commissioner explain the basis for current STAR configurations and processes, and outline actions planned in response to the audit recommendations. The response identified compensating controls that have been implemented in lieu of having background checks completed. However, the identified non-disclosure agreements, GSA Rules of Behavior, and on-line security courses are not compensating access controls. Procedures cited in the Commissioner's response define responsibilities but do not prevent access by individuals or monitor their use of STAR or its data. We therefore reaffirm the need to ensure compensating controls are established until background checks have been completed.

IMPROVEMENTS NEEDED IN MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS FOR PBS' STAR SYSTEM REPORT NUMBER A040159/P/T/R05006

INTRODUCTION

The Public Buildings Service (PBS) implemented the System for Tracking and Administering Real Property (STAR) in 1997 to provide a means to track and manage the government's real property assets and to store inventory data, billing data, building data, customer data, and lease information. As such, STAR is a mission-critical system managed by the Office of the PBS Chief Information Officer that supports management aspects of real property space management, including identification of all building space, daily management of 22,000 assignments, and monthly billing for all property to its client Federal agencies. PBS' real property inventory consists of over 8,900 buildings and 340 million square feet of office and warehouse space for which Federal agencies pay PBS approximately $6 billion per year in rent. STAR provides PBS realty specialists and portfolio managers the capability to input and update business data and direct access to business data supporting the management of space and customer billing records. Beyond initial capabilities, STAR has been expanded to support the security function in the FPS mega-centers, to bill other Federal agencies for rent, to provide management information for GSA and other Federal managers, and to exchange data with other systems through the PBS Data Gateway System.

The Office of Inspector General (OIG) Information Technology (IT) Audit Office issued a report on STAR in March 2000[1]. At that time, we found that: (1) STAR modifications were still underway to respond to numerous user concerns, resolve software problems, and provide additional key capabilities; (2) PBS remained heavily dependent upon the sole-source contractor for day-to-day operation of STAR and implementation of technical solutions; and (3) PBS experienced difficulty in implementing and maintaining a project management structure and system development methodology to ensure the proper development of system capabilities and implementation of system control processes. We also reported that STAR management and control weaknesses needed to be resolved to complete systems development and migrate STAR to a stable operation and maintenance system life cycle phase.

In October 2002, our office also issued a report on the PBS Systems Development Center (SDC)[2], which included an assessment of STAR management through the SDC. PBS had attempted to address ongoing difficulties with developing and managing efficient and effective IT systems by implementing the SDC. The SDC approach did not successfully meet PBS' project management goals for its systems. PBS established an Application Review Panel to review and monitor projects, including STAR, for development, enhancement, and implementation as well as recommend project changes to reflect PBS business processes.

[1] PBS Needs to Complete STAR Development and Implement Management and System Controls to Fully Realize Improved Capabilities, Report Number A995010/P/T/R00013, dated March 31, 2000.

[2] The Systems Development Center Has Not Successfully Met PBS Project Management Goals, Report Number: A020043/P/T/R03001, dated October 31, 2002.

Objectives, Scope, and Methodology

The objective of our review was to assess how well the STAR system is meeting management and user requirements, and the effectiveness of system security controls. Our review focused on STAR project management, security, quality assurance, testing, and system controls. We analyzed key documentation, including the Security Plan, Business Continuity Plan, Risk Assessment, security testing and evaluation reports, certification and accreditation documentation, results of vulnerability scanning, and PBS enterprise architecture documentation. We met with a wide range of PBS officials, contract personnel, and STAR users, including the STAR Program and Project Managers; security officials; contractors responsible for system development, database administration, and computer operations; and persons responsible for data accuracy. We also reviewed the STAR Master Plan dated October 2002, Post-Implementation Review dated August 2001, and Business Case for fiscal years (FY) 2005 and 2006. STAR was concurrently reviewed and incorporated in the FY 2004 review of GSA's IT Security Program required by the Federal Information Security Management Act (FISMA). Our office recently issued two separate reports on STAR security. FY 2004 Office of Inspector General Review of GSA's Information Technology Security Program, Report Number: A040179/O/T/F04015, dated September 27, 2004, provided the results of our FISMA review, which included our assessment of security controls for nine systems, including STAR, across GSA's Services, Staff Offices, and Regions. Detailed results for our FISMA control tests for STAR were reported subsequently in FY 2004 Office of Inspector General Information Security Review of the System for Tracking and Administering Real Property, Report Number: A040179-10/O/T/F05014, dated January 5, 2005. With our FISMA review, we have previously provided specific results of our technical vulnerability scanning and detailed findings on security controls for STAR to the GSA Office of the Chief Information Officer (CIO) and to PBS management.

To assess managerial, operational, and technical controls for the system, we relied on: (1) applicable statutes, regulations, policies, and operating procedures such as: the GSA Information Technology (IT) Security Policy, CIO P 2100.1B, November 2004; the Government Performance Results Act of 1993; Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, December 2003; FIPS Publication 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, April 1981; the CIO Council's A Practical Guide to the Federal Enterprise Architecture, Version 1.0, February 2001; Federal Information Systems Control Audit Manual (FISCAM), January 1999; Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, November 28, 2000; OMB Circular A-11, Preparation, Submission, and Execution of the Budget, July 2004; Guide for Developing Security Plans for Information Technology Systems, National Institute of Standards and Technology (NIST) Special Publication 800-18, December 1998; Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, January 2002; Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34, June 2002; OMB FY 2004 Reporting Instructions for the Federal Information Security Management Act; and the GSA CIO's IT procedural guides on password generation and protection, security incident handling, conducting risk assessments, developing contingency and configuration management plans, security test and evaluation, access control, auditing and monitoring, and certification and accreditation. We also referenced the Government Accountability Office's Standards for Internal Control in the Federal Government, Property Management Systems Requirements - Checklist for Reviewing Systems Under the Federal Financial Management Improvement Act, December 2001; Executive Guide, Measuring Performance and Demonstrating Results for Information Technology Investments, March 1998; and Assessing Reliability of Computer-Processed Data, October 2002; as well as the GSA Financial Statement Audit, PricewaterhouseCoopers, 2004.

We performed our audit work in GSA's Central Office, the National Capital Region (NCR), and contacted users in the New England Region (Region 1), Northeast and Caribbean Region (Region 2), the Mid-Atlantic Region (Region 3), Southeast Sunbelt Region (Region 4), and the Heartland Region (Region 6). We performed our audit work between March and December 2004, in accordance with generally accepted government auditing standards. The scope of our audit did not include a detailed analysis of the data within STAR or the accuracy of that data. Our audit scope also did not include a review of PBS' contractual practices used in procuring STAR or the overall acquisition process.

RESULTS OF AUDIT

The System for Tracking and Administering Real Property (STAR) was developed to provide improved functional capabilities for many of the Public Buildings Service's (PBS) business processes. Management, operational, and technical controls for the system, however, need to be strengthened to better provide necessary functional capabilities in support of PBS' business processes. Recent organizational, business, and system changes have challenged PBS' ability to manage STAR efficiently and effectively, and in a manner consistent with enterprise architecture goals for information technology (IT). While PBS has taken steps to improve the collection and reporting of performance measures through the STAR business case, additional steps are needed to establish and achieve system-specific measures and goals for long-term efficiency and effectiveness. Further, PBS has not yet completed a comprehensive data dictionary for STAR that can be leveraged across the organization to effectively support business functions. System security weaknesses requiring action include the need to: (1) complete background checks for contractors supporting STAR prior to providing them with access to the system and its resources; (2) capture additional detail with audit trails to support investigations should normal system operations cease; (3) reassess whether additional protection for system interfaces is warranted; and (4) develop a more comprehensive approach to monitoring risks with the system. Taking steps to strengthen management, operational, and technical controls for STAR will better enable PBS to ensure long-term success for this mission-critical system by providing the information needed to effectively manage its real property assets.

Careful Assessment of STAR Functionality and Performance Measures Is Essential in Light of Business Process Changes

Since the STAR system was implemented in 1997, PBS has undergone changes in key business processes, which have resulted in the need to change the system's functionality. Modifications to STAR have not been guided by an enterprise architecture, or an IT road map for PBS, and the STAR business case was only recently modified to more adequately collect and report on established performance improvement goals. Consequently, adequate performance metric data for STAR is needed for PBS to better direct the system towards target performance improvements. To determine whether STAR system investments are meeting business and system requirements, system-specific performance measures must be first identified and then monitored. Further, the data dictionary for STAR is not comprehensive enough to adequately describe system data or information provided by the system in support of PBS business processes. A more thorough assessment of STAR requirements and its performance is needed to assist PBS in establishing and meeting its long-term needs for this critical system in support of changing business processes.

System Functionality Changes Have Not Been Consistent with a Target Architecture

Changes in functionality required for STAR, including the way PBS computes rent charges, continue to challenge the system's development and operations efforts. These changes have also affected PBS' ability to develop and implement a "to be" or target enterprise architecture. With STAR, PBS purchased a commercial-off-the-shelf (COTS) package called the Permanent Record of Managed Property Transactions (PROMPT) system from AT&T System Leasing Corporation as the base for the system. Since 1997, PBS has spent approximately $75 million to implement and enhance STAR, and current lifecycle costs through fiscal year (FY) 2009 estimate the system will eventually cost PBS over $150 million. When acquired, PROMPT and other COTS products considered by PBS did not perform needed billing functions, which led PBS to invest $4.8 million to develop new billing functionality for STAR. A subsequent decision to change PBS' billing processes to more closely align with lower private sector costs resulted in additional modifications of STAR to allow for billing based on rentable space rather than from usable space. This change had the unforeseen effect of causing customer rent bills to fluctuate even though the tenant's space assignments had not changed. Thus, to better meet customer needs, PBS has recently decided to develop new billing functionality in the Occupancy Agreement (OA) Tool, to replace STAR's billing capabilities. The resulting duplication in billing system functionality does not support GSA's goals for enterprise architecture and IT capital planning and investment.

The 2002 STAR Master Plan addresses the need to review billing policies in STAR to identify validity, citing fluctuating rent bills as a major complaint, and notes several development activities for improving billing functionality. The Master Plan presents the results of a vision and strategy, a technology baseline, a system assessment, and a business case analysis for improving PBS systems that support the need to improve the systems that support the lease management, property management, construction and renovation management, business management, and customer service management processes. The FY 2006 business case for STAR identifies that Federal agencies rely on the system to hold data regarding building availability, space details, and billing information, and that the client billing record (CBR) is one of the modules within the system used as a tool for PBS employees. With this change, monthly reports will be run to identify whenever STAR updates to its building inventory require changes to information within the OA Tool for billing purposes. However, neither the STAR Master Plan nor the Business Case includes plans to integrate or otherwise eliminate redundant modules when PBS moves to bill from the OA Tool. While PBS plans to begin billing from the OA Tool in April of 2005, this will require that: (1) occupancy agreements be put in place for a large number of tenants and (2) data reconciliation be performed between STAR and the OA Tool. For occupancy agreements that are not in place prior to this date, PBS will need to bill customers from the CBRs that currently reside within STAR. When new occupancy agreements are entered into the OA Tool and finalized, edit checks for STAR will be performed. Using the proposed new billing process, CBRs will remain in STAR to enable management of the building inventory. After the transition to the new OA Tool, STAR and the OA Tool could contain duplicate data that may require reconciliation. PBS officials advised that they are developing but have not formalized or integrated plans for reducing duplicate processes and data in STAR and the OA Tool. In such a dynamic business environment, it is critical that the development of mission-critical systems like STAR be guided by an enterprise architecture that defines business strategy and processes, data needed to manage the business, applications, and technology used to provide the data, while reflecting the impact of ongoing changes in business functions and supporting IT capital planning and investment decisions.

Performance Goals Are Not Yet Specific to STAR and Have Not Been Consistently Monitored

PBS has taken steps to improve the collection of and reporting on performance measures for STAR despite significant changes to PBS business, system, and organizational processes.

However, while STAR had performance goals and measures tied to GSA's strategic goals, none of the performance goals or measures for STAR are tied specifically to system performance. Further, the STAR Business Case for the FY 2005 budget submission indicated that data had not been captured and none was reported for the strategic goals of achieving responsible asset management and of providing best value for customer agencies and taxpayers. In January 2005, subsequent to our audit fieldwork, PBS updated its FY 2006 business case for STAR by adding specific planned performance improvement goals, actual performance improvement results, planned performance metrics, and actual performance metric results for its FY 2003 and FY 2004 strategic goals, information previously omitted from the business case. Again, recently reported results were not tied to STAR performance. As a result, information is not available to assess how well the system is meeting user needs and system requirements.

According to the 2002 GSA IT Strategic Plan, GSA’s vision for information technology is to design, build, and operate a customer-focused, agile, and highly secure set of services and applications to enable the agency to deliver what customers want efficiently and effectively. Related strategic goals are intended to provide managers with a yardstick to measure achievement in operating their programs more efficiently and effectively. The Government Performance and Results Act (GPRA) of 1993 requires Federal agencies to focus on defining missions, setting goals, measuring performance, and reporting accomplishments to include demonstrated improvements in performance measurement. Performance goals are to be objective, quantifiable, and measurable in order to provide a basis for comparing actual results against established goals. Additionally, for assets like STAR that are in operation, the Office of Management and Budget (OMB) requires that agencies demonstrate how close actual annual operating and maintenance costs are to the original life-cycle cost estimates, and whether the level or quality of performance and capability meets the performance goals and continues to meet agency and user needs. Not meeting GPRA and OMB requirements for STAR has left PBS unable to measure long-term efficiency and effectiveness of this mission critical system. System-specific performance goals are needed to ensure that STAR system investments meet specified user needs and functional requirements, and PBS needs to routinely monitor performance metric data to ensure that it meets established performance improvement goals.

Data Dictionary Is Not Comprehensive Enough to Adequately Describe Information Supporting PBS Business Processes

A comprehensive STAR data dictionary accessible across PBS business lines has not yet been completed and therefore cannot be leveraged across the organization to more effectively use the system. This condition relates directly to a finding we reported in our March 2000 report, where we identified that PBS had not completed a data mapping of PROMPT and PBS information systems to compare relationship diagrams detailing the different parts of the organization (business entities), the relationships between information used by the different business entities, and the specific data elements and attributes contained in the information. Further, database documentation provided for PROMPT at that time was not as complete and thorough as that used by PBS, because PROMPT did not capture many of the data elements used by PBS. Currently, PBS utilizes the Business Information Solution (BIS) database as an enterprise-wide data dictionary. The BIS database is composed of data from four systems, including STAR, and is intended to provide a business level understanding of the data, rules, values and distribution of data contained in the BIS database tables and columns. However, the tables and columns for STAR lack a number of key components needed to more effectively use the system.

BIS tables identify the types of data the table contains and what the data is used for. Specific information identified for tables includes rules, which define the entity relationship; AKA (Also Known As), which is used to identify the enterprise business standard name or another common business name by which this attribute is known; the system physical name, which supplies users with the authoritative source for the data in the column; distributed to, which identifies if data is distributed to another system as well as the name of the system and the physical table and entity business name in the receiving system; and the distributed from, which identifies if data is distributed from another system as well as the name of the system and the physical table and entity business name of the sending system.

For the 106 **tables** within the STAR data dictionary:

- 50% do not identify "rules" for data content;
- 75% do not identify other names ("AKAs") used for the table;
- 65% do not identify where the data in the table is "distributed to;" and
- 97% do not identify where the data in the table is "distributed from."

Columns are the specific data fields within the tables, as described above, and include similar information specifically related to each data field.

For the 1,852 **columns** within the STAR data dictionary making up the tables:

- 93% do not identify the "value" portion of the data field;
- 57% do not identify where the data is "distributed to;"
- 98% do not identify where the data is "distributed from;"
- 88% do not identify "rules" for data content; and
- 71% do not identify other names ("AKAs") used for the data field.

Further, the data dictionary for STAR does not specify optional and required data that is dependent on other data, nor does it identify the range of values, source, and authorization for access for each of the data elements. For the majority of data elements, the dictionary does not indicate which application programs use the data in specific fields. This is especially useful when trying to determine how STAR uses the data and which elements of STAR data are exchanged with subscribing systems[3], such as Pegasys, the Occupancy Agreement Tool, and the Operational Data Store. The STAR data dictionary also does not group the data elements, making it difficult to present the information in recognizable units that would facilitate user understanding of its contents.

In 2001, a post-implementation analysis[4] for STAR completed by Booz·Allen & Hamilton Inc. concluded that the lack of links to other systems, in addition to a lack of historical data and difficulty accessing data, have resulted in a STAR system that does not efficiently meet user data access needs. Further, the analysis recommended that PBS overcome the inconsistent use of

[3] Subscribing systems are systems that interface with STAR. Almost all of these interfaces are conducted through the Data Gateway.

[4] STAR Post-Implementation Analysis Final Report, dated August 20, 2001.

terms and data fields that contribute to data inaccuracy for the system. An effective data dictionary would accurately and completely define data contained in the database and indicate which application programs use the data so that, when a data structure is contemplated, a list of the affected programs can be generated. A detailed data dictionary for STAR would also help to simplify database modification, reduce data redundancy, and increase data reliability. In addition to the benefits already discussed, improvements with the STAR data dictionary would facilitate information sharing and better enable PBS to more efficiently and effectively promote its IT investments.

System Risk Must Be Managed with Appropriate Security Controls

We identified several weaknesses with STAR security controls that could lead to system vulnerabilities or unnecessary risks. With our FY 2004 Federal Information Security Management Act (FISMA) review[5], which identified specific security weaknesses including results from system vulnerability scans, we previously provided these findings to the Office of the GSA Chief Information Officer[6] and PBS management in an effort to provide prompt feedback on security concerns for GSA's systems. The report, through a detailed analysis of STAR security controls, identified specific risks that need to be addressed. First, National Agency Check and Inquiries Credit background checks, as required by the GSA IT Security policy for contractors before being provided access to critical system and data resources, have not yet been completed, leaving the system vulnerable to unauthorized access to or modification of system functionality and data resources. Second, audit trails for STAR lack sufficient detail, which may negatively affect PBS' ability to efficiently and effectively recover from the cessation of normal system operations. Third, sensitive data may not be adequately protected during transmission to and from STAR, raising the potential for this information to be compromised or to fall into the hands of unauthorized users. Finally, system security certification and accreditation (C&A) documents that we reviewed for STAR did not address all security controls as required by GSA-CIO's IT Security Program.

Background Checks Have Not Been Completed for Contractors Supporting STAR

Contractors working with STAR have not received required background checks before being allowed access to the STAR system and its data, as required by the GSA IT Security Policy. The PBS contract with the system developer has only recently been modified to require that background checks be completed. Because employee access to and use of STAR data affects GSA's mission, operations, and efficiency of service, STAR positions have been identified as Government public trust positions. For this reason, PBS employees and contractors who access STAR must undergo a suitability investigation (background check) and receive public trust certification. If contractor staff is permitted to access the system prior to the completion of appropriate background screening, compensating controls to mitigate the associated risk need to be in place. While PBS has requested the required background checks for existing and new

[5] FY 2004 Office of Inspector General Review of GSA's Information Technology Security Program, Report Number: A040179/O/T/F04015, September 27, 2004.

[6] FY 2004 Office of Inspector General Information Security Review of the System for Tracking and Administering Real Property, Report Number: A040179-10/O/T/F05014, January 5, 2005.

contractors developing or operating STAR, compensating controls should be established until this process is completed.

Audit Trails Lack Sufficient Detail

If normal operations of the STAR system ceased, the system's audit trail documentation may not adequately support after the fact investigations, or provide sufficient detail to trace user actions. Thus, PBS may be unable to efficiently and effectively detect and recover from potential security incidents caused by administrative or user errors, irregularities, or security flaws and weaknesses. The STAR Security Plan confirms that there are no audit trails for SQL database IDs or UNIX operating system IDs and that UNIX only retains owner, date, and time information for each file. For every STAR database table in which a row can be updated or inserted by a batch job, the table stores the batch job name along with the date and time of the last update, but the limited audit logging captured by STAR is not detailed enough to identify the changes made, or easily resolve changes made in error.

While a proposal to introduce server management and monitoring improvements for STAR was prepared by the PBS Infrastructure Division in May 2003, little progress has been made toward the proposed improvements. PBS noted that modifications to capture and retain all data element changes and to provide historical data to research changes to transactions would be a major and potentially costly modification. PBS advised that they were waiting to make a decision about how to better incorporate audit logging within the system until related guidance from the National Institute of Standards and Technology (NIST) is finalized. The GSA "IT Security Procedural Guide, Auditing and Monitoring, CIO-IT Security-01-08," dated April 27, 2001, states that auditing and monitoring is an all inclusive security concept that encompasses a wide range of security activities and provides valuable input into security processes such as security test and evaluation, certification and accreditation, and risk assessment. Audit trails must be improved if they are to provide an effective control that offers a snapshot of the state of the system at any given time to better enable PBS to detect incidents and recover from the cessation of normal operations.

Transmission of Sensitive Data May Not Be Adequately Protected

PBS has decided not to encrypt data transmissions from the system that are behind the firewall that protects GSA's wide area network. However, the STAR Security Plan states that unauthorized access to, loss, misuse, or modification of the sensitive data in STAR could be expected to have severe or catastrophic adverse effects on GSA and other agency operations, missions, functions, and assets. According to the Federal Information Processing Standards Publication 74, protection of sensitive data during transmission may be necessary to maintain the confidentiality and integrity of the information represented by the data, and encryption of this sensitive information within Federal computer networks is needed. The sensitivity level for the confidentiality, availability, and integrity of STAR data is considered high, and PBS has recognized that in the hands of wrongdoers, sensitive STAR data on agency buildings, locations, physical features, and numbers of employees could be used to facilitate hostile acts against the United States Government, resulting in loss of human life and destruction of Government facilities of grave proportions. The memorandum of agreement between STAR and the Data

Gateway identifies that certain security measures are required to protect STAR data both in storage and during transfer. System interfaces are required to meet the level of security described in the STAR Security Plan, including coordination of periodic administrative risk evaluations; maintenance of continuous operational controls, technical controls, secure data handling practices, and other physical and technical safeguards; and maintenance of trusted behavior. Without encrypting sensitive data as it is passed between STAR and the Data Gateway and between the Data Gateway and other GSA systems, STAR data may not be adequately protected since GSA has over 17,600 users with access to the Agency's wide area network. A careful reassessment of the need to encrypt data transmitted within the GSA network should be considered to preserve confidentiality and integrity of STAR's sensitive data.

Key Components of System Security Have Not Been Comprehensively Addressed With Certification and Accreditation of Controls

Several components of STAR security do not comprehensively address risks as required in GSA-CIO's IT Security Program, even though PBS has completed a risk assessment, security plan, and contingency plan, and has identified that security weaknesses for STAR are being documented and tracked in a system-level Plan of Action and Milestones (POA&M). A certification and accreditation (C&A) was performed for the system on May 9, 2003, and a POA&M has been developed and is being used to help manage risk with the system. PBS security officials have also implemented a vulnerability scanning program to identify and mitigate system vulnerabilities. However, it is not clear specifically which security controls will be monitored on a periodic basis, and the system Risk Assessment did not include a risk level matrix to prioritize risks, threats, and vulnerabilities for STAR. Additionally, the system Security Plan did not identify and discuss the full range of operational, managerial, and technical controls, such as documenting rules and procedures for system interconnections; backup procedures; procedures for verifying that default passwords have been changed; procedures for reviewing access control lists to identify and remove users who have left the organization or whose duties are no longer required to access the system; and the laws, regulations, and policies affecting STAR in terms of requirements for confidentiality, integrity, and availability. The Business Continuity Plan has been completed, but it did not include critical contingency planning steps necessary to comprehensively address risks, such as information on the reconstitution phase for the plan and established agreements for the alternate site, completion of a business impact analysis, inclusion of detailed information on the alternate site, and identification of testing and maintenance schedules. As a result, STAR and its data may be exposed to undue risks if PBS does not take steps to more comprehensively address potential system threats and vulnerabilities. Necessary management and operational controls for the system would be strengthened by a more robust certification and accreditation process.

Recommendations

In order to strengthen managerial, operational and technical controls for the STAR system, we recommend that the Commissioner, Public Buildings Service, work with the PBS-CIO to ensure that:

1. STAR provides necessary business line management information through:

a. System enhancements, which are consistent with enterprise architecture goals.
b. System-specific performance measures for identifying and monitoring progress with meeting established goals and system requirements.
c. A complete system data dictionary designed to capture the comprehensive nature of information in STAR and more effectively leverage the system across the organization.

2. Adequate security controls are in place to manage risks with STAR by:
   a. Completing necessary background checks for contractor staff as required by the GSA IT Security Policy and implementing compensating controls, as necessary, until this process is completed.
   b. Enhancing the system's audit trails to provide an effective control for capturing a snapshot of information at any given time to better enable system monitoring and recovery.
   c. Reassessing the risk of not encrypting the transmission of sensitive STAR data.
   d. Updating the system risk assessment, security plan, and business continuity plan to more comprehensively address potential system threats and vulnerabilities.

Management Comments

In his response to our draft report, the PBS Commissioner provided comments on specific audit findings and recommendations, which are included in their entirety as Appendix A. The response includes explanations for current STAR configurations and processes and outlines actions that are, or will be, taken in response to the audit findings, and generally concurs with the recommendations. Brief segments of the March 31, 2005 response are included here for each finding and recommendation.

Regarding the reported need for careful assessment of STAR functionality in light of business process changes, PBS advised in part that they; "have updated the process documentation to reflect that the Enterprise Architect will be actively involved at the beginning of requirements gathering and will ensure adherence to the Enterprise Architecture throughout the Software Development Lifecycle (SDLC)." Also, PBS "will review the current performance measures with the Business Lines, as well as Business Analytics Division and strengthen our system-specific performance measures for identifying and monitoring progress with meeting established goals and system requirements." With the data dictionary, they "will review listed deficiencies and input the missing information as identified in the IG Audit Report."

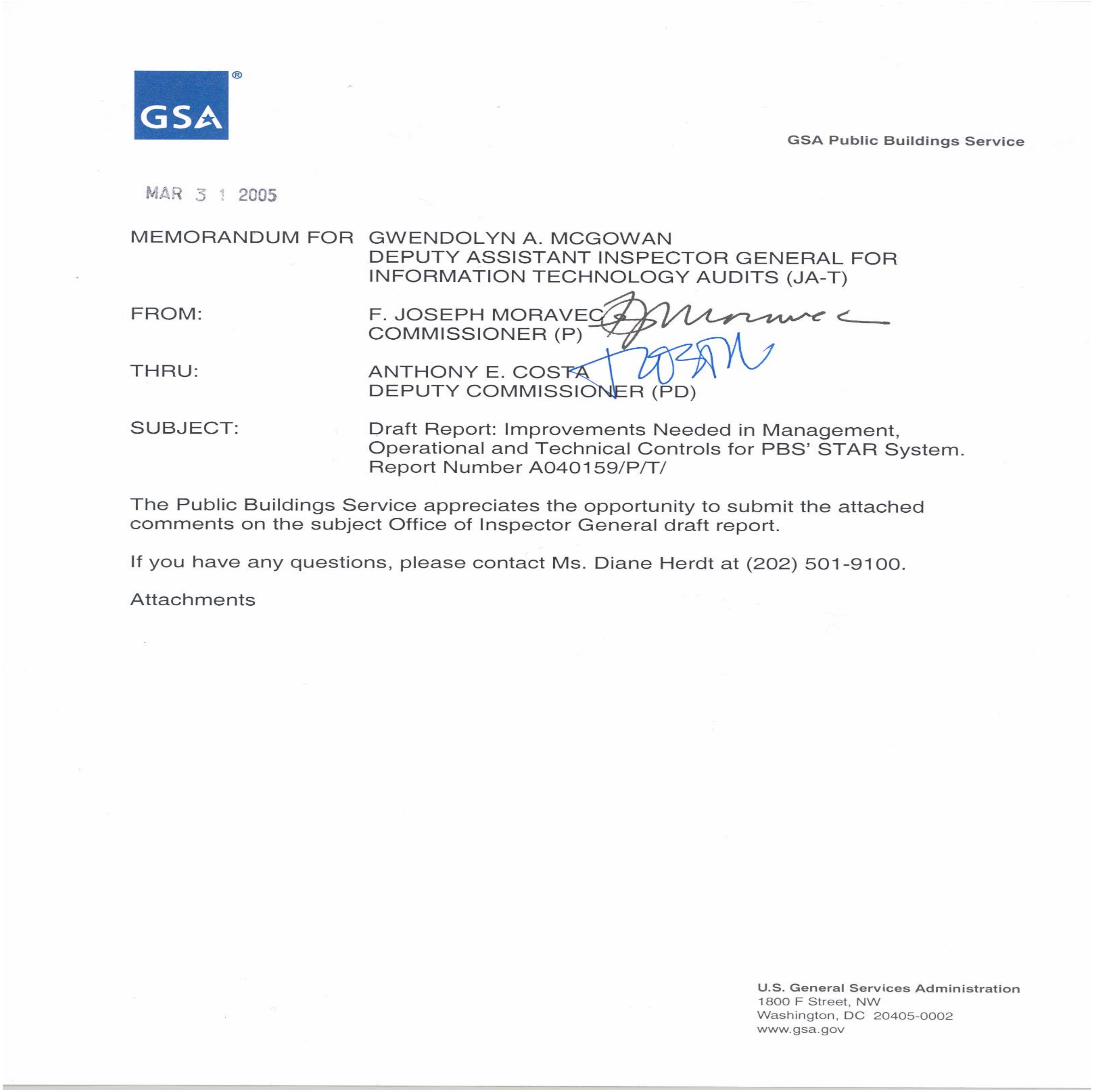
In response to managing system risk with appropriate security controls, the Commissioner stated that: "Background investigation paperwork has been submitted for all STAR developer contractor personnel and OPM has completed action on about 30% of these investigations. Current status of completion has been communicated with the IG. The STAR SSP, Section 3.1.3 Interim Access to STAR and Non-Disclosure Agreements details the compensating controls that are in place to enable development contractors to access STAR data pending completion of a background check." We note that procedures cited in the commissioner's response define responsibilities but do not prevent access by untrustworthy individuals or monitor uses of STAR data by individuals. Regarding audit trails, PBS responded that they will: "seek independent verification and impact analysis for implementing audit features based upon a review of STAR's current audit trail capability, the IG audit findings, the NIST 800-53, and FIPS 200. A significant financial investment may be required to bring STAR into full compliance with the NIST Guidelines coupled with the audit recommendations. This investment may require software enhancements to STAR and the acquisition of additional auditing and monitoring tools for the development and production environments." PBS stated that: "The PBS CIO Office will reassess and make a risk-based decision regarding the use of encryption to protect the confidentiality and integrity of sensitive STAR data that is exchanged behind the GSA firewall." The Commissioner also stated that: "In future updates to the system security plan, risk assessment, and business continuity plan; we will more comprehensively address potential system threats and vulnerabilities. We will also include a risk level matrix in the STAR Risk Assessment to prioritize the risks, threats, and vulnerabilities for STAR; and we will update the ESC Business Continuity Plan to include the critical contingency planning steps."

Internal Controls

As discussed in the Objectives, Scope, and Methodology section of this report, the objective of our review was to assess how well the STAR system is meeting management and user requirements, and the effectiveness of system security controls. Thus, we analyzed the sufficiency of STAR systems development, project management, system requirements, and system controls. The Results of Audit and Recommendations sections of this report state in detail the need to strengthen specific managerial, operational, and technical controls with STAR. The scope of our audit did not include a detailed analysis of the data within STAR or the accuracy of that data. Our audit scope also did not include a review of PBS' contractual practices used in procuring STAR or the overall acquisition process.

IMPROVEMENTS NEEDED IN MANAGEMENT,
OPERATIONAL, AND TECHNICAL
CONTROLS FOR PBS' STAR SYSTEM
REPORT NUMBER A040159/P/T/R05006

PBS RESPONSE TO DRAFT REPORT



GSA Public Buildings Service

MAR 3 1 2005

MEMORANDUM FOR GWENDOLYN A. MCGOWAN
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INFORMATION TECHNOLOGY AUDITS (JA-T)

FROM: F. JOSEPH MORAVEC
COMMISSIONER (P)

THRU: ANTHONY E. COSTA
DEPUTY COMMISSIONER (PD)

SUBJECT: Draft Report: Improvements Needed in Management, Operational and Technical Controls for PBS' STAR System. Report Number A040159/P/T/

The Public Buildings Service appreciates the opportunity to submit the attached comments on the subject Office of Inspector General draft report.

If you have any questions, please contact Ms. Diane Herdt at (202) 501-9100.

Attachments

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

After reviewing the draft report, the following section contains PBS' responses to the outlined recommendations. Our comments are organized and summarized in response to the Recommendations section of the Executive Summary and are in blue color.

Recommendations

In order to strengthen managerial, operational and technical controls for the STAR system, we recommend that the Commissioner, Public Buildings Service, work with the PBS-CIO to ensure that:

1. STAR provides necessary business line management information through:

   a. System enhancements, which are consistent with enterprise architecture goals.

[In Blue] We believe all STAR enhancements are consistent with Enterprise Architecture goals. In particular, during requirements development for billing from the Occupancy Agreement (OA) Tool, we have specifically addressed elimination of redundant modules, an EA goal. For example, the current STAR functions include the PBS inventory of all buildings and space, an inventory of all leases including space and rental payments and our billing system. To reduce the duplicate data entry we are taking steps to eliminate the redundancy through the dual business process redesign and the system. The OA tool enhancements specifically will provide for these improvements as well as increase our data accuracy.

We also continue to keep our Enterprise Quality Program (EQP) updated. This includes updating the Project Management Plan (PMP), Configuration Management Plan (CMP), Independent Validation and Verification Plan (IV&VP), and the Quality Assurance Plan (QAP). We have updated the process documentation to reflect that the Enterprise Architect will be actively involved at the beginning of requirements gathering and will ensure adherence to the Enterprise Architecture throughout the Software Development Lifecycle (SDLC).

   b. System-specific performance measures for identifying and monitoring progress with meeting established goals and system requirements.

[In Blue] Currently, the performance measures for STAR are business-specific and have been consistently monitored. As outlined in our 300B report, STAR has very specific strategic goals listed. For FY 2005 and 2006, they include:

- Achieve responsible Asset Management
- Provide best value for customer agencies and taxpayer
- Operate efficiently and effectively.

In addition, we submit monthly reports on earned value on the project to the Office of the GSA CIO. We also track Helpdesk calls and monitor for system changes.

For the future, for system-specific performance measures, we will measure and track the following from the 2005 GSA Information Technology Measures:

- Maintain full Certification and Accreditation (C&A)
- % of system weaknesses completed on time or on schedule
- Rated highly for Business Case by OMB
- Rated highly for Enterprise Architecture by OMB

We will review the current performance measures with the Business Lines, as well as Business Analytics Division and strengthen our system-specific performance measures for identifying and monitoring progress with meeting established goals and system requirements. We will review with the Business the possibility of adding system availability or system uptime measures.

c. A complete system data dictionary designed to capture the comprehensive nature of information in STAR and more effectively leverage the system across the organization.

[In Blue] We will review listed deficiencies and input the missing information as identified in the IG Audit Report.

2. Adequate security controls are in place to manage risks with STAR by:

   a. Completing necessary background checks for contractor staff as required by the GSA IT Security Policy.

[In Blue] Background investigation paperwork has been submitted for all STAR developer contractor personnel and OPM has completed action on about 30% of these investigations. Current status of completion has been communicated with the IG. The STAR SSP, Section 3.1.3 Interim Access to STAR and Non-Disclosure Agreements details the compensating controls that are in place to enable development contractors to access STAR data pending completion of a background check.

   b. Enhancing the system's audit trails to provide an effective control for capturing a snapshot of information at any given time to better enable system monitoring and recovery.

[In Blue] The current Audit Trail sufficiently provides an effective control for capturing a snapshot of information at any given time to better enable system monitoring and recovery. The NIST Special Publication 800-53 "Recommended Security Controls for Federal Systems" was published in February 2005 and is intended to provide guidance to federal agencies until the publication of FIPS 200, "Minimum Security Controls for Federal Information Systems" (projected for publication December 2005). These minimum security controls once published will be mandatory for all major Federal systems and PBS will comply.

The focus of the audit recommendation is the organizations “ability to efficiently and effectively recover after cessation of normal activities.” The ability to recover from the cessation of normal activities is heavily reliant on a system’s back up and recovery procedures. STAR back up and recovery procedures include nightly back ups to the STAR server and to an off site location. STAR is also backed up on a weekly cycle. Currently these back-ups are maintained off site for a four-week cycle

We will seek independent verification and impact analysis for implementing audit features based upon a review of STAR’s current audit trail capability, the IG audit findings, the NIST 800-53, and FIPS 200.

A significant financial investment may be required to bring STAR into full compliance with the NIST Guidelines coupled with the audit recommendations. This investment may require software enhancements to STAR and the acquisition of additional auditing and monitoring tools for the development and production environments. These tools once acquired must be “tuned” to monitor and establish the appropriate alerts. Additionally individuals must be trained to operate the tools and monitoring procedures must be developed. Because of the potential cost in terms of software development and requirement to potentially acquire additional monitoring tools for the development and production environments as well as the requirement to train individuals to run these tools multiple analyses are required. These analyses are needed to identify what transactions should be maintained and how long they should be maintained, processing and storage requirements, user interface requirements, and what tool sets and training are required. Documentation will also need to be developed for end users and production personnel.

c. Reassessing the risk of not encrypting the transmission of sensitive STAR data.

[In Blue] PBS has implemented virtual private network (VPN) connectivity to better ensure the confidentiality and integrity of sensitive data transmitted outside the GSA firewall. We disagree with the portion of the finding that focuses on encrypting data that is passed behind the GSA firewall and to include data that is passed between STAR and the Data Gateway. Encryption only protects data in the transmission and storage data states. The GSA Firewall protects data in our databases (without encryption) it should be sufficient to protect data that is transferred from one system to another, as long as the systems are behind the firewall. Additionally, a review of Chapter 5, paragraph 7 of the GSA IT Security Policy (CIO P 2100.1B, November 5, 2004) confirms that all sensitive but unclassified information that is transmitted outside the GSA firewall shall be encrypted. While STAR contains SBU data, the boundaries for the STAR to Data Gateway interface are all within the PBS ESC and are all behind the GSA firewall. The 17,600 users who access GSA’s area wide network do not have access to the data as it is passed from STAR to the Data Gateway and then on to other systems.

The STAR batch process occurs at about 10 PM, the online system is locked out to allow for batch processing. The STAR batch process includes the data transfer to the Data Gateway. Users cannot access STAR during the batch process or the Data Gateway interface during this process. Data Gateway does not have any application users. The exchange that occurs between STAR and the Data Gateway is controlled through the use of a password and access rights. Data accessed in the data gateway is read access only and does not compromise the integrity of Star data.

Implementation of encryption based upon the NIST encryption standards may involve significant costs and adversely impact the performance for STAR and each of the downstream systems that receive sensitive STAR data.

The goal of information security is to deny unauthorized access to information resources in an economically efficient manner. In determining a security strategy for a system or the organization, the PBS CIO must determine the correct balance between mitigating appropriate risks and expending resources.

The PBS CIO Office will reassess and make a risk-based decision regarding the use of encryption to protect the confidentiality and integrity of sensitive STAR data that is exchanged behind the GSA firewall.

d. Updating the system security plan, risk assessment, and business continuity plan to more comprehensively address potential system threats and vulnerabilities.

[In Blue] STAR is scheduled for recertification and reaccredidation during FY 2006. A risk assessment will be conducted during FY 2006 as part of the recertification and reaccredidation process. The STAR SSP and Business Continuity Plan will also be updated.

In future updates to the system security plan, risk assessment, and business continuity plan; we will more comprehensively address potential system threats and vulnerabilities. We will also include a risk level matrix in the STAR Risk Assessment to prioritize the risks, threats, and vulnerabilities for STAR; and we will update the ESC Business Continuity Plan to include the critical contingency planning steps.

IMPROVEMENTS NEEDED IN MANAGEMENT,
OPERATIONAL, AND TECHNICAL
CONTROLS FOR PBS' STAR SYSTEM
REPORT NUMBER A040159/P/T/R05006

REPORT DISTRIBUTION

	Copies
Commissioner, Public Buildings Service (P)	3
Chief Information Officer, Public Buildings Service (PG)	2
Chief Information Officer (I)	2
PBS Management Control and Audit Liaison, Office of the PBS Chief Financial Officer (PF)	1
Assistant Inspector General for Auditing (JA and JAO)	2
Deputy Assistant Inspector General for Real Property Audits (JA-R)	1
Audit Follow-up and Evaluation Branch (BECA)	1
Audit Planning Staff (JAN)	1
Administration and Data System Staff (JAS)	1
Assistant Inspector General for Investigations (JI)	2