GENERAL SERVICES ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

Audit of PBS's Controls over Security of Building Information in Online Environments

Report Number A070216/P/R/R10003
March 31, 2010

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: March 31, 2010

Reply to Attn of: R. Nicholas Goco
Deputy Assistant Inspector General
for Real Property Audits (JA-R)

Subject: Audit of PBS's Controls over Security of Building Information in Online Environments
Report Number A070216/P/R/R10003

To: Robert A. Peck
Commissioner, Public Buildings Service (P)

This report presents the results of our review of the controls PBS has implemented to protect sensitive building information in online environments. There is a concern that unrestricted construction documents pose a vulnerability that could be exploited by terrorists or other criminal elements. Public Buildings Service (PBS) policy includes the following principles regarding sensitive building information: 1) only give the information to those who have a "need-to-know"; 2) keep records of who received the information; and 3) safeguard the information during use and destroy it properly after use. In September 2008, the GSA Office of Inspector General (OIG) issued a review of PBS's controls over the security of paper and removable media. During the course of the audit fieldwork, the OIG became aware of PBS's use of electronic project management software (e-PM) applications, as far back as 1998. Many of these applications, which contain sensitive but unclassified building information, did not appear to be under the purview of either the GSA Office of the Chief Information Officer (OCIO) or the PBS OCIO.

Consequently, on September 3, 2008, the OIG notified senior PBS management of our initial concerns in this area and initiated a separate review focusing on the security controls over sensitive but unclassified building information in online information systems. Overall, this review disclosed that PBS needs to place a greater emphasis on security over its sensitive building information in online environments. In particular, PBS needs to develop and implement a security strategy for existing e-PM applications and any that may be employed in the future. PBS also needs to conduct more security awareness training to raise the level of attention to online data security within the organization.

If you have any questions regarding this report, please contact me or R. Nicholas Goco, Deputy Assistant Inspector General for Real Property Audits, on (202) 219-0088.

Susan P. Hall

Susan P. Hall
Audit Manager
Real Property Audit Office (JA-R)

Audit of PBS's Controls over Security of Building Information in Online Environments

Report Number A070216/P/R/R10003

Audit of PBS's Controls over Security of Building Information in Online Environments

Report Number A070216/P/R/R10003

EXECUTIVE SUMMARY

Purpose

The objective of our review of the Public Buildings Service's (PBS) efforts to protect sensitive building information in online environments was to determine if PBS has implemented managerial, physical, and technical controls to effectively mitigate risks inherent to sensitive but unclassified building information in online systems.

Background

A priority for the General Services Administration (GSA) is the physical protection of Federal employees, the visiting public, and its facilities. There is a concern that unrestricted construction documents pose a vulnerability that could be exploited by terrorists or other criminal elements. Public Buildings Service (PBS) policy includes the following principles regarding sensitive building information: 1) only give the information to those who have a "need-to-know"; 2) keep records of who received the information; and 3) safeguard the information during use and destroy it properly after use. This policy encompasses security requirements for the dissemination of electronic documents, including physical facility information such as building designs, construction plans, specifications, and any other information considered a security risk. PBS employees are required to protect sensitive building data using techniques such as data encryption, appropriate sanitization/disposal of media, and incident handling procedures.

In September 2008, the GSA Office of Inspector General (OIG) issued a review of PBS's controls over the security of paper and removable media. During the course of audit fieldwork, the OIG became aware of PBS's use of electronic project management software (e-PM) applications, as far back as 1998. Many of these applications, which contain sensitive but unclassified building information, did not appear to be under the purview of either the GSA Office of the Chief Information Officer (OCIO) or the PBS OCIO. Consequently, on September 3, 2008, the OIG notified senior PBS management of our initial concerns in this area and initiated a separate review focusing on the security controls over sensitive but unclassified building information in online information systems.

Results in Brief

The Public Buildings Service needs to improve its controls over sensitive building information in online environments to reduce the risk of inappropriate disclosure of information that may result in harm to people or property. In particular, electronic project management technologies and groupware, such as intranet websites, present vulnerabilities that need to be addressed through stronger controls.

In the late 1990s, PBS project teams began using e-PM technologies as a tool to enable PBS and its construction contractors to electronically share project data. However, PBS has not included these systems under the purview of its security program or ensured compliance with Federal Information Security Management Act (FISMA) requirements. For example, PBS policy essentially charged construction project managers with security responsibilities without support from either the GSA Office of the Senior Agency Information Security Officer or the PBS OCIO. Further, the contractual agreements with the providers of the e-PM solutions in our audit sample did not include language to enforce IT security requirements or provide for testing rights and only one specified data archival requirements. PBS is currently conducting a pilot for a new enterprise-wide e-PM system. Many of the security related concerns raised in this review appear to be addressed in the contractual language for the new enterprise-wide e-PM system. However, data remains vulnerable until the new enterprise-wide e-PM system is successfully implemented.

A related issue that also needs to be addressed is that of controls over sensitive but unclassified data shared generally within the GSA environment through regional web pages. The multiple instances of inadequately protected sensitive data encountered during the OIG's testing of PBS's groupware/intranet controls indicate a lack of awareness among PBS personnel regarding information security principles.

Overall, PBS needs to place a greater emphasis on security over its sensitive building information in online environments. In particular, PBS needs to develop and implement a security strategy for existing e-PM applications and any that may be employed in the future. PBS also needs to conduct more security awareness training to raise the level of attention to online data security within the organization.

Recommendations

We recommend that the PBS Commissioner

1) Work within the framework of the GSA OCIO security program to develop and implement a security strategy for e-PM applications. The security strategy should address

    a) The identification and inventory of e-PM applications currently in use that are not under the purview of a security program;

    b) Security control testing on existing e-PM applications and procedures for ongoing monitoring and correction;

    c) IT security roles for existing PBS e-PM applications as required by GSA CIO P 2100.1E and identify FISMA points-of-contact for the FISMA points-of-contact list published by the GSA OCIO;

    d) Procedural guidance to the Contracting Officer, Contracting Officer Technical Representative, Project Manager and Project Executive related to IT contracts or

contracts containing IT, considering PBS 3490.1A, GSA CIO P 2100.1E, and other GSA CIO procedural guides;

e) Policies and procedures for PBS OCIO oversight during the entire system lifecycle for any project using electronic project management tools; and

f) The amendment of existing contracts, where feasible, related to the acquisition of electronic project management services and development of boilerplate contract language that includes

   i) Current applicable GSA, PBS, and Federal laws, regulations and policy;
   ii) Security control assessment rights;
   iii) Requirements for the inclusion of security requirements in subcontracts; and
   iv) Project data archival requirements.

2) Develop and conduct additional security awareness training for project management and contracting personnel, especially for those with significant security responsibilities. Include a focus on requirements for extranet based e-PM applications where appropriate, a review of PBS sensitive but unclassified information policy, and instruction on the protection of sensitive data in PBS groupware/intranet environments.

Audit of PBS's Controls over Security of Building Information in Online Environments

Report Number A070216/P/R/R10003

INTRODUCTION

Background

A priority for the General Services Administration (GSA) Public Buildings Service (PBS) is the physical protection of Federal employees, the visiting public, and its facilities. There is a concern that unrestricted construction documents pose a vulnerability that could be exploited by terrorists or other criminal elements. GSA must balance security concerns with the need for building data to be accessible to those authorized to conduct Government business.

In order to reduce the exposure to possible attacks or threats to GSA-controlled facilities, PBS issued in March 2002, GSA Order, PBS 3490.1 (PBS 3490.1) entitled, "Document security for sensitive but unclassified paper and electronic building information." The principles of this policy are: 1) only give the information to those who have a "need-to-know"; 2) keep records of who received the information; and 3) safeguard the information during use and destroy it properly after use. This policy defined security requirements for the dissemination of electronic documents, including physical facility information such as building designs, construction plans, specifications, and any other information considered a security risk. On June 1, 2009, PBS updated its sensitive but unclassified policy with GSA Order PBS 3490.1A, entitled "Document security for sensitive but unclassified building information." The revised policy requires PBS employees to adhere to encryption, sanitization/disposal, and incident handling requirements.

In September 2008, the GSA Office of Inspector General (OIG) issued a review of PBS's controls over the security of paper and removable media entitled "Audit of PBS's Controls over Security of Building Information, Report Number A070216/P/R/R08005." The OIG found that the implementation of the controls to meet the requirements for safeguarding sensitive building information on hardcopy and removable media across PBS varied widely; oversight practices were inconsistent; and many contracts did not include the contractor's responsibility to use reasonable care to protect sensitive building information. The review also disclosed that while the majority of PBS staff interviewed were aware of PBS's sensitive but unclassified policy, few had received formal training in the requirements and how to implement them.

During the course of audit fieldwork, the OIG became aware of PBS's use of electronic project management software (e-PM) applications, as far back as 1998. Many of these applications, which contain sensitive but unclassified building information, did not appear to be under the purview of either the GSA Office of the Chief Information Officer (OCIO) or PBS OCIO. These tools were being provided by various software vendors and application service providers. Consequently, on September 3, 2008, the OIG notified senior PBS management of our initial concerns in this area and initiated a separate review focusing on the security controls over sensitive but unclassified building information in online information systems.

Objective, Scope and Methodology

The objective of our review of PBS's efforts to protect sensitive building information in online environments was to determine if PBS has implemented managerial, physical, and technical controls to effectively mitigate risks inherent to sensitive but unclassified building information in online systems.

To accomplish this audit objective we performed fieldwork primarily in PBS's National Office, National Capital Region, Southeast Sunbelt Region, and Mid-Atlantic Region. During fieldwork, we performed the following tasks:

- Obtained background information including Office of Management and Budget Circulars and memoranda; National Institute of Standards and Technology (NIST) publications; the Federal Information Security Management Act (FISMA); GSA Information Technology (IT) Security Policy, (GSA CIO P 2100.1D, dated June 21, 2007 and CIO P 2100.1E, dated July 2, 2009); and prior GSA Office of Inspector General audit reports.

- Reviewed e-PM vendor documentation including stated security features, such as access controls for data and functions.

- Obtained internal PBS documentation including PBS FISMA Certification and Accreditation (C&A) documentation.

- Interviewed PBS National and Regional officials to determine what controls they have in place to ensure the security of sensitive building information in online systems.

- Interviewed GSA senior agency information security officials.

- Examined GSA's groupware environment to identify sensitive but unclassified data, as well as links to this data that may exist therein, that may be vulnerable to unauthorized access.

- Reviewed six judgmentally selected PBS construction projects using electronic project management (e-PM) tools[1] provided by various software vendors and application service providers to determine

    - If the projects contained sensitive but unclassified information, and the nature of that information;
    - The basis for e-PM vendor selection;
    - The actions PBS project teams took to ensure the e-PM application/system met applicable GSA/PBS security requirements;
    - If contract language stated responsibilities for safeguarding GSA data, including sensitive but unclassified information;

[1] One of these e-PM tools was being used for over 50 projects and had over 900 users.

- If contract language provided GSA vulnerability testing rights; and
- The procedures for data archival at project completion.

The audit work was conducted between September 2008 and December 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESULTS OF AUDIT

The General Services Administration (GSA) Public Buildings Service (PBS) needs to improve its controls over sensitive building information in online environments to reduce the risk of inappropriate disclosure of information that may result in harm to people or property. In particular, electronic project management (e-PM) technologies and groupware, such as intranet websites, present a vulnerability that needs to be addressed through stronger controls.

Although PBS has used e-PM technologies since at least 1998, the systems have been used and acquired independent of the PBS security program. As a result, PBS has not had the security in place to ensure that there are adequate safeguards over sensitive building information. The use of these e-PM technologies grew out of a need to electronically share data between PBS and its contractors for construction projects. Prior PBS policy placed responsibility for the security essentially with its construction project managers; however, no support, training, or guidance was provided to assist in implementing security controls. Further, most contractual agreements with the providers of the e-PM solutions in our audit sample did not include language to enforce IT security requirements, such as requiring the systems to be FISMA compliant or provide for testing rights. These clauses are necessary to ensure the security and availability of vital building information.

PBS is currently conducting a pilot for a new enterprise-wide e-PM tool that will be physically located in an internal data center. Many of the security related concerns raised in this review appear to be addressed in the contractual language for the new enterprise-wide e-PM system. However, until the new system is fully implemented, the risk that sensitive but unclassified data is not adequately protected still exists for e-PM applications.

In addition to the e-PM technologies issue, we found multiple instances of inadequately protected sensitive data during our testing of PBS's groupware/intranet controls, such as building plans in regional web sites. This suggests a lack of awareness among PBS personnel regarding basic sensitive information security principles.

Overall, PBS needs to place a greater emphasis on security over its sensitive building information in online environments. In particular, PBS needs to develop and implement a security strategy for existing e-PM applications and any that may be employed in the future. PBS also needs to conduct more security awareness training to raise the level of attention to online data security within the organization.

Although PBS has used e-PM technologies since 1998, the systems have been used and procured independent of PBS's security program.

The e-PM tools are secured web-based applications that are used for 1) team communication and document management; 2) work flow and process automation, and; 3) project management of design and construction activities. Also known as "Construction Project Extranets," these technologies offer communication platforms, project management functionalities, and hosted collaboration spaces for architecture, engineering, and construction projects, which are usually hosted by application service providers. By using e-PM applications, all project team members

have access to the same information at the same time, from any location, which improves project timeliness, accuracy, and efficiency. Standardization allows for efficient training, optimization of tool utilization, and consolidation of all project information for better program management. Additionally, a complete audit trail of communications, activities, and dates is generated, reducing claim risks.

At PBS, a reduction in administrative tasks, improvement in request for information turnaround time, and the ability to measure project performance based on the national measures for budget and schedule have all been noted as benefits of e-PM technologies. Although PBS has no formal national policy regarding e-PM technology, regional executives have been encouraged to advocate their use and PBS encourages its project managers to take advantage of the many benefits e-PMs afford.

Even though PBS project teams have used many e-PM technologies for over a decade, the systems have not been under the purview of a security program. Prior PBS policy assigned e-PM security to system users; however, no support or guidance was set up to implement security requirements. Further, the e-PM applications were acquired using multiple arrangements without input or oversight by IT security staff. As a result of the lack of oversight, security control testing and system monitoring were not performed and Federal Information Security Management Act (FISMA) compliance was not addressed. In addition, security requirements were not addressed in contracts in cases where contractors provided e-PM software.

Prior policy assigned security responsibilities to users.

Until its revision, the March 2002 GSA Order, PBS 3490.1 (PBS 3490.1) entitled, "Document security for sensitive but unclassified paper and electronic building information," placed responsibility for e-PM security with system users; essentially construction project managers as well as other project team members. According to the policy that remained in effect until June 2009, authorized users of project extranets for e-PM applications that transfer sensitive but unclassified building information were required to verify and certify to the Government Contracting Officer that physical and technical GSA security requirements, as determined by the PBS CIO, were met.

Based on the policy, the authorized users had to determine the adequacy of the technical security controls in the e-PM products under consideration. However, additional guidance or technical support was not set up to assist the users. For example, PBS had not established a list of approved e-PM vendors, specific guidance on required e-PM security features, or procedures for PBS CIO involvement in the e-PM acquisition process to facilitate this verification and certification process.

In addition, none of the project managers, contracting officers, or project executives we interviewed during our review received training beyond the standard periodic GSA CIO IT Security Awareness Training for GSA Employees. As was previously reported in the September 2008 OIG report (Report Number A070216/P/R/R08005), the majority of PBS staff interviewed were aware of PBS's sensitive but unclassified policy, but few had received formal training in the requirements and how to implement them. Consequently, there are no personnel with

significant security responsibilities assigned to these extranet-based applications that have the advanced technical security training required to fulfill these security responsibilities. Given this situation, none of the project teams in our sample confirmed that the required verifications and certifications were performed.

In June 2009, the policy was revised. The new policy, PBS 3490.1A, requires PBS associates to adhere to encryption, sanitization/disposal, and incident handling. However, the new policy does not specifically discuss the IT security responsibilities for e-PM applications. According to the PBS OCIO, it is now responsible for the security of these applications.

Multiple sources for e-PM applications create oversight issues.

The e-PM applications being used by PBS were provided through multiple arrangements. In some cases, PBS acquired and owned the application. In other cases, the e-PM software being used on a project was provided by one of the contractors on the projects, such as the architect/engineer, the construction manager, or the general contractor. Since these e-PM systems were not procured through an information technology vehicle, they had no visibility in GSA's annual Office of Management and Budget Exhibit 53, which identifies GSA's IT investment portfolio.

While certain e-PM systems were under PBS's control and all the e-PM software packages had stated security features, the PBS OCIO was not consulted by the project teams for any of the projects in our audit sample prior to the implementation of the e-PM tools. In some cases, project personnel were assisted by knowledgeable internal business line technical support, but there was no formal process for their involvement. In addition, internal business line technical support did not get involved if an architectural/engineering firm or construction manager owned the e-PM system, as was the case in three of our six sample projects.

Since the applications were not under the purview of a security program, oversight and security measures were not implemented and FISMA was not addressed.

While PBS officials have solicited information regarding the use of e-PM solutions in the regions, the identification and security controls testing and monitoring of these applications has not occurred. As of July 29, 2008, neither the GSA OCIO nor the PBS OCIO had an inventory of the e-PM applications being used at PBS. Given that neither office was involved in the selection or acquisition of the e-PM systems, they could not determine whether the e-PM systems meet applicable agency security requirements. As of December 8, 2009, security officials for these e-PM systems had not been assigned. Without these systems being identified, tested, and monitored, PBS does not have adequate assurance that the risks inherent to systems containing sensitive building information have been kept to an acceptable level.

A central tenet to providing security for systems is assurance of confidentiality, integrity, availability, and accountability of systems through risk-based management. Security control testing and monitoring would be part of the controls for risk-based management, however, these controls were not implemented for existing e-PM systems. Vulnerability testing conducted by the GSA CIO, as described in GSA CIO P 2100.1E, usually includes vulnerability scanning of

operating systems, databases, and web applications on a quarterly basis, or when significant new vulnerabilities potentially affecting the system are identified and reported. Although some of the internally supported e-PM applications have implemented vulnerability scanning since we initiated this review, none of the externally supported or owned e-PM systems have conducted these tests. Since the effectiveness of security controls in these existing applications are not routinely monitored and evaluated against known vulnerabilities and configuration issues, PBS's sensitive building information could be vulnerable to unauthorized access.

Many of the e-PM applications used at PBS were not compliant with FISMA. FISMA requires each agency to develop, document, and implement an agency-wide information security program that provides information security for the information and information systems that support the agency, including those provided or managed by another agency, contractor, or other source. In addition to other requirements, this program must include a risk assessment addressing unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems, a system security plan, security awareness training, periodic control testing, a remedial action process to address any deficiencies in the information security policies, procedures, and practices of the agency, an incident response process, and a business continuity plan. Office of Management and Budget Memorandum M-07-19, "FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," dated July 25, 2007, states that FISMA applies to services which are fully or partially provided, including agency hosted, outsourced, and software-as-a-service (SaaS) solutions. In support of these requirements, GSA CIO P 2100.1E requires that every IT system, both Government and contractor operated, must undergo a security control review annually[2].

Since initial deployment, existing e-PM applications continue to operate without FISMA certification and accreditation. As of December 8, 2009, security officials for these e-PM systems, as outlined in GSA CIO P 2100.1E, have not been assigned. Although the contract for the new enterprise-wide e-PM system requires the offeror to work with PBS on the e-PM FISMA certification and accreditation (C&A), the existing e-PM systems may still be at risk.

When e-PMs were provided by contractors, the contracts did not include security requirements.

When e-PM software being used on a project is provided by one of the contractors on the project, such as the architect/engineer, the construction manager, or the general contractor, the contract should address requirements associated with the confidentiality, integrity, and availability of sensitive building data in the application. At the project level, PBS system owners, along with the contracting officer and system program managers, share in the responsibility for ensuring IT security requirements are included in IT contracts or contracts including IT requirements, according to GSA CIO P 2100.1E. Although two of the projects sampled in our review referenced PBS sensitive but unclassified information policy, none of the sampled contracts contained direct references to GSA CIO IT security policy, which imposes a robust set of control requirements to protect GSA's information and information systems. Without GSA CIO IT

[2] Annual reviews must use the current version of NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," and CIO IT Security 04-26, "FISMA Implementation." Note that NIST SP 800-53 Revision 2 was released in December 2007.

security requirements specified in existing e-PM contracts, providers of e-PM solutions or support may not provide appropriate safeguards to prevent unauthorized users from accessing sensitive building information.

Four control areas were assessed when reviewing contractual agreements as part of this audit: GSA CIO IT security policy adherence, security control testing rights, archival data availability, and requirements for the proper handling of sensitive but unclassified building (SBU) data. For the six sample projects in this review, none of the contracts included GSA IT security policy requirements or security control testing rights. Only one contract established data archival requirements. Only two contracts contained sensitive but unclassified data handling requirements as defined by PBS policy. As a result, the existing e-PM systems have not been properly tested for the required technical, operational, and managerial controls necessary to ensure the confidentiality of sensitive data and may still pose a security risk.

Only one of the six contracts sampled during our review utilized an in-house e-PM application on an internally owned and administered hardware and software platform[3]. After the audit fieldwork identified the application, PBS conducted security testing on the application. PBS has not conducted security testing on the other five sample projects, which are either fully or partially supported by non-GSA resources. None of these contracts provide PBS with security control testing rights. Consequently, GSA does not have a contractual right to conduct testing where the risk to sensitive building data is at its highest. GSA CIO P 2100.1E requires GSA task orders and contracts to allow the government or its designated representative (i.e. third party contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of the security controls; including, but not limited to, documentation review, server configuration review, vulnerability scanning, physical data center reviews, and operational process reviews. Until the existing contracts are amended to include security control testing rights for PBS, the effectiveness of the security controls in externally supported e-PM applications is uncertain.

Construction project data must be available after a project is complete to address any outstanding legal issues, including potential litigation, and to support future efforts regarding the facilities involved in the project. Additionally, data loss can arise from disaster, hardware failure, sabotage, etc. Proper data archival helps to address these risks. However, four out of five of the externally supported e-PM contracts in our sample did not have archival requirements for project data.

The September 2008 OIG report observed that many contracts did not include the contractor's responsibility to use reasonable care to protect sensitive building information. In the current review, only two of the sampled projects' contracts referenced PBS sensitive but unclassified data protection policy. As such, the contracts for the other e-PM solutions currently utilized in PBS construction projects did not have the PBS sensitive but unclassified data handling requirements necessary to provide the awareness and accountability needed to protect sensitive building information.

[3] This e-PM tool was being used for over 50 projects and had over 900 users.

Although PBS's new e-PM system should correct many of these risks, until its development is complete and adopted by all projects, risks will remain.

PBS is in the pilot phase of a new enterprise-wide e-PM system implementation that should address Federal, GSA CIO and PBS security requirements. The contract for the new system includes provisions for the certification and accreditation of this application according to FISMA requirements. The contract for the new e-PM system also appears to be in compliance with GSA CIO IT security policy and related procedural guides, including vulnerability testing, and PBS sensitive but unclassified policy requirements. The new enterprise-wide e-PM contract addresses archival requirements and PBS will control physical custody of the system. The new enterprise-wide e-PM contract language addresses both PBS security requirements and GSA CIO security policy. Furthermore, these requirements are carried over to subcontractors. This new system was expected to be available for use on construction projects funded through the American Recovery and Reinvestment Act of 2009. However, the system's development has yet to be completed and fully implemented. Until the new e-PM system is fully adopted by all of the PBS project teams and the use of other e-PM applications ceases, the security vulnerabilities will remain and PBS will need to develop a security strategy to mitigate these risks.

Sensitive data found on GSA internal web-sites indicates the need for additional security training and awareness.

PBS 3490.1A notes, "Disseminators of SBU building information are responsible for providing the first line of defense against misuse," and requires employees to have security training on the procedures in the order. GSA policy also requires all GSA personnel and contractors to receive annual IT security awareness training as part of its overall security program. Those personnel with significant security related responsibilities must receive the applicable training necessary to carry out their duties as well. A lack of familiarity with GSA's security policy may lead to individuals inadvertently making sensitive data available to unauthorized users.

Vulnerabilities identified during OIG control testing suggest a lack of awareness regarding what composes sensitive building information and proper use of the applicable technical, managerial, and operational security controls necessary to protect such information. During control testing conducted in May 2007 through July 2007 by the GSA OIG, access control weaknesses were identified in a number of databases, including a PBS Project Information Portal (PIP). This portal included sensitive design documents, housing plans, floor plans, financial data, and photographs of PBS construction projects. Corrective security measures have since been implemented.

As part of this review, further control testing was performed in November 2008 on PBS internal groupware and intranet sites. This control testing identified vulnerabilities regarding sensitive building information. Examples of the data found included building plans with secure functions identified, a report on the structural analysis of a Federal building, links to the Customer Profile System (CPS), and banking information for contractors. The OIG immediately provided PBS officials with the relevant details, including the regional *Insite*[4] websites examined, and the

[4] *InSite* is a federal government computer system, for official use only, by GSA employees and contractors with network access through GSA systems. *Insite* is not accessible to the general public.

system or application concerned. Out of 35 total applications/links/web pages identified that may potentially be storing or processing sensitive but unclassified building data, 24 (68.6 percent) did not have any further access controls established, outside of a user having access to GSA *Insite*. As such, these 24 applications/links/web pages were not restricting access based on the concept of "need-to-know." In response to our testing results, PBS officials have emphasized to employees the need to protect sensitive building information and corrective measures have been implemented or are in progress at this time to reduce or eliminate these vulnerabilities. These incidents suggest the need for additional and continuing information security awareness training.

CONCLUSION

PBS needs to improve the security over sensitive building information in online environments to reduce the risk of inappropriate disclosure of information that may result in harm to people or property. In particular, PBS needs to emphasize security for electronic project management (e-PM) technologies, groupware and intranet websites.

While e-PM technologies have been in use for years, PBS project personnel have been using and acquiring these applications independent of the PBS security program. As a result, PBS has not had the security in place to ensure that these applications have adequate technical security controls to safeguard sensitive building information. Although PBS has made considerable progress toward the implementation of an enterprise-wide e-PM system that will manage many of the risks highlighted in this report, security risks will continue with existing e-PM deployments as well as any that are used in the future. Given this situation, PBS needs to work with the GSA OCIO to develop and implement a security strategy for current and future e-PM applications and PBS also needs to ensure that its enterprise-wide e-PM application meets security requirements.

With regard to groupware, the multiple instances of inadequately protected sensitive data encountered during the OIG's testing of PBS'S groupware/intranet controls suggests a lack of awareness among PBS personnel regarding basic sensitive but unclassified information security principles, such as only providing information to those individuals with a legitimate need for access. As such, PBS needs to conduct more security awareness training to raise the level of attention to online data security within the organization.

RECOMMENDATIONS

We recommend that the PBS Commissioner

1) Work within the framework of the GSA OCIO security program to develop and implement a security strategy for e-PM applications. The security strategy should address

    a) The identification and development of the inventory of e-PM applications currently in use that are not under the purview of a security program;

b) Security control testing on existing e-PM applications and procedures for ongoing monitoring and correction in order to manage the risk of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the sensitive data contained in these applications or the unavailability of the applications themselves;

c) IT security roles for existing PBS e-PM applications as required by GSA CIO P 2100.1E and identify FISMA points-of-contact for the FISMA points-of-contact list published by the GSA OCIO;

d) Procedural guidance to the Contracting Officer, Contracting Officer Technical Representative, Project Manager and Project Executive related to IT contracts or contracts containing IT, considering PBS 3490.1A, GSA CIO P 2100.1E, and other GSA CIO procedural guides;

e) Policies and procedures for PBS OCIO oversight during entire system lifecycle for any project using electronic project management tools; and

f) The amendment of existing contracts, where feasible, related to the acquisition of electronic project management services and development of boilerplate contract language that includes

   i) Current applicable GSA, PBS, and Federal laws, regulations, and policy;
   ii) Security control assessment rights;
   iii) Requirements for the inclusion of security requirements in subcontracts; and
   iv) Project data archival requirements.

2) Develop and conduct additional security awareness training for project management and contracting personnel, especially to those with significant security responsibilities. Include a focus on requirements for extranet based e-PM applications where appropriate, a review of PBS sensitive but unclassified policy, and instruction on the protection of sensitive but unclassified data in PBS groupware/intranet environments.

MANAGEMENT COMMENTS

Management generally concurred with the report recommendations.

INTERNAL CONTROLS

As discussed in the Objective, Scope, and Methodology section of this report, the review focused on whether PBS has adequate controls in place to protect sensitive building information in online environments. Related management control issues are discussed in the context of the review findings.

Audit of PBS's Controls over Security of Building Information in Online Environments

Report Number A070216/P/R/R10003

Appendix A

Management Response

GSA

GSA Public Building Service

MAR 3 1 2010

MEMORANDUM FOR R. NICHOLAS GOCO
DEPUTY ASSISTANT INSPECTOR GENERAL
FOR REAL PROPERTY AUDITS (JA-R)

FROM: ROBERT A. PECK
COMMISSIONER
PUBLIC BUILDINGS SERVICE (P)

SUBJECT: Draft Audit Report: Audit of PBS's Controls over Security of Building Information in Online Environments Report Number A070216/P/R/R09###, February 25, 2010

The Public Buildings Service (PBS) appreciates the opportunity to review and comment on the subject draft audit report. PBS generally agrees with the recommendations presented in the report and will prepare a corrective action plan, where feasible and practical, to address these findings upon receipt of the final audit report.

If you or your staff have any questions or require additional information, please contact Diane Herdt, PBS Chief Information Officer, on (202) 501-9100.

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

Audit of PBS's Controls over Security of Building Information in Online Environments

Report Number A070216/P/R/R10003

Appendix B

Report Distribution

	Copies
Commissioner, Public Buildings Service (P)	1
Office of the Chief Information Officer (IS)	1
Regional Administrator, National Capital Region (WA)	1
Regional Administrator, Southeast Sunbelt Region (4A)	1
Regional Inspector General for Auditing (JA-W, JA-4)	2
Regional Inspector General for Investigations (JI-W, JI-4)	2
Deputy Assistant Inspector General for Information Technology Audits (JA-T)	1
Office of Inspector General (J)	4
Assistant Inspector General for Auditing (JA, JAO)	2
Assistant Inspector General for Investigation (JI)	1
Director, Internal Control & Audit Division (BEI)	1