

GENERAL SERVICES ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

**AUDIT OF PBS'S CONTROLS OVER
SECURITY OF BUILDING INFORMATION
REPORT NUMBER A070216/P/R/R08005
SEPTEMBER 30, 2008**



U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: September 30, 2008

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

Subject: Audit of PBS's Controls Over Security of Building Information
Report Number A070216/P/R/R08005

To: David L. Winstead
Commissioner, Public Buildings Service (P)

This report presents the results of our review of the controls PBS has implemented to protect sensitive building information. After the Alfred P. Murrah Federal Building bombing, PBS issued guidance to control access to sensitive, but unclassified, paper and electronic building information. Our review found that although detailed policy has been in effect for several years, PBS needs to improve its implementation of controls over sensitive building information to reduce the risk of inappropriate disclosure.

Overall, implementation of the controls to meet the requirements for safeguarding sensitive building information varied widely. Also, PBS project managers' and contracting officers' oversight of the security policies was inconsistent. The variations and inconsistencies were especially evident in the contracts, since many contracts did not incorporate the contractor's responsibility to use reasonable care to protect sensitive building information. While the majority of PBS staff interviewed during our review was aware of the key policy for safeguarding sensitive building information, few had received formal training on the requirements and how to implement them. PBS is currently in the process of revising the applicable policy and may be able to use this as an opportunity to address many of the issues identified by our review.

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
REPORT NUMBER A070216/P/R/R08005**

TABLE OF CONTENTS

	<u>PAGE</u>
EXECUTIVE SUMMARY	i
INTRODUCTION	1
Background	1
Objective, Scope, and Methodology	2
RESULTS OF AUDIT	4
Controls over Security Requirements are not Consistently Applied Across the Regions	4
PBS Security Requirements are Often not Included in Construction Contracts	9
Inclusion of Security Requirements Varied Between Contract Types	10
Contractors Adhered to Security Requirements	13
Contracts Should Include Requirements for Safeguarding Sensitive Building Information	14
Formal Training for the Project Team is Needed	14
PBS is Currently Drafting Revisions to GSA Order, PBS 3490.1	15
CONCLUSION	15
RECOMMENDATIONS	16
MANAGEMENT COMMENTS	16
MANAGEMENT CONTROLS	16
APPENDICES	
Management Response	A-1
Report Distribution	B-1

**AUDIT OF PBS'S CONTROLS OVER
SECURITY OF BUILDING INFORMATION
REPORT NUMBER A070216/P/R/R08005**

EXECUTIVE SUMMARY

Purpose

The audit objective was to determine whether the Public Buildings Service (PBS) has adequate controls in place to protect sensitive building information.

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 growing concern that unrestricted construction documents pose a vulnerability that could be exploited by terrorists or other criminal elements. In March 2002, GSA enhanced its policy on securing building information by issuing GSA Order, PBS 3490.1 (PBS 3490.1) entitled, "Document security for sensitive but unclassified paper and electronic building information." The objectives of the policy were: 1) only give the information to those who have a need to know, 2) keep records of who got the information, and 3) safeguard the information during use and destroy it properly after use.

Since May 2007, there have been two examples of security breaches over Sensitive but Unclassified (SBU) information, where sensitive but unclassified building drawings were found in public places. In another instance, a database control weakness was identified in a PBS Project Information Portal containing SBU information.

Results in Brief

PBS needs to improve its implementation of controls over sensitive building information to reduce the risk of inappropriate disclosure of sensitive building information that may result in harm to people or property. Overall, implementation of the controls to meet the requirements for safeguarding sensitive building information varied widely. The oversight practices of PBS project managers and contracting officers to implement PBS security policies were inconsistent. The inconsistent implementation was especially evident in the contracts, as many contracts did not include the contractor's responsibility to use reasonable care to protect sensitive building information. While the majority of PBS staff interviewed was aware of PBS 3490.1, few had received formal training on the requirements and how to implement them. PBS is currently in the process of revising the security requirements in PBS 3490.1 and may be able to use this as an opportunity to address many of the issues identified by our review.

Recommendations

PBS needs to take steps to ensure that controls are in place to properly protect sensitive building information. These steps include incorporating PBS 3490.1 requirements directly into the boilerplate Solicitation for Offers and contracts for architect and engineering, construction, and lease construction contracts; requiring contractors to include PBS 3490.1 requirements in their subcontracts; and developing a course of action to be taken when contractors do not fulfill their contractual obligations regarding the protection of SBU information. PBS should also ensure officials are provided training on PBS 3490.1. This training should include encryption software applications available to PBS project personnel. To ensure that PBS 3490.1 requirements are being followed by PBS project teams, a system of controls should also be implemented.

**AUDIT OF PBS'S CONTROLS OVER
SECURITY OF BUILDING INFORMATION
REPORT NUMBER A070216/P/R/R08005**

Introduction

Background

A priority for the General Services Administration (GSA) is the physical protection of Federal employees, the visiting public, and its facilities. After the Alfred P. Murrah Federal Building bombing, GSA and other agencies reviewed GSA's construction and security criteria to find ways to prevent such an occurrence in the future. There is a growing concern that unrestricted construction documents pose a vulnerability that could be exploited by terrorists or other criminal elements. GSA must balance these legitimate security concerns with the reality that its buildings and related data should be accessible to the public and that excessive security restrictions might hamper competition for GSA projects.

In order to reduce the exposure to possible attacks or threats to GSA-controlled facilities, the Public Buildings Service (PBS) issued a PBS Instructional Letter PBS-IL-01-3 entitled "Dissemination of Sensitive but Unclassified Paper and Electronic Design and Construction Documents" dated July 30, 2001. Sensitive but Unclassified (SBU) information was defined by the policy as drawings, plans, and specifications for new or current GSA-controlled space, produced specifically as contract and solicitation documents for construction purposes, or material used to define structural analysis for facilities, for installation of security systems, or any documents that would disclose information about security guards or security systems of any kind. The objectives of this policy were to 1) diminish the potential that construction or security related documents (either paper or electronic) will be used by a person or persons with an interest in causing harm to persons or property, and 2) not impede the availability of necessary information to those with legitimate needs, such as the professional design community, contractors, professional schools and forums, and states, cities, and towns where GSA has facilities.

In March 2002, GSA enhanced its policy by issuing GSA Order, PBS 3490.1 (PBS 3490.1) entitled, "Document security for sensitive but unclassified paper and electronic building information." The objectives of the policy were essentially the same as above, with the principles of this policy being: 1) only give the information to those who have a need to know, 2) keep records of who got the information, and 3) safeguard the information during use and destroy it properly after use. This policy defined security requirements for proper document labeling, keeping records of those obtaining SBU documents, notification of proper disposal of building documents, and dissemination of electronic documents. As of October 2007, efforts were underway to revise the policy to take into account PBS's reorganization, new governmental policy, and technical advancements.

Since May 2007, there have been two examples of security breaches over SBU information. In May 2007, sensitive architectural drawings for the construction of the new Los Angeles

Courthouse were discovered in a Phoenix, Arizona cemetery. And in July 2007, preliminary expansion drawings for the Ysleta Border Station were found in a dumpster behind an Austin, Texas television studio. Also, during control testing conducted in May 2007 through July 2007 by the GSA Office of Inspector General, access control weaknesses were identified in a number of databases, including a PBS Project Information Portal. This portal included sensitive design documents, housing plans, floor plans, financial data and photographs of PBS construction projects.

Lapses in security over SBU information are not confined to the Federal Government. Recently, detailed SBU documents regarding the reconstruction efforts at Ground Zero were discovered in trash bins on two occasions. In the first instance, a homeless man found a set of SBU drawings for the construction of the Freedom Tower in a trash bin outside a restaurant in New York City. After this story made the newspapers, two salvage experts contacted the news agency and turned over 300 pounds of sensitive building information related to construction projects in and around Ground Zero, which they found in a dumpster. The New York Port Authority Inspector General is investigating the matter.

Objective, Scope, and Methodology

The audit objective was to determine whether PBS has adequate controls in place to protect sensitive building information. To accomplish this audit objective we performed fieldwork primarily in GSA's National Office, National Capital Region, Southeast Sunbelt Region, and the Greater Southwest Region. The scope of this review was limited to paper and removable media. An additional review of the protection of sensitive building information in online environments is currently in progress. Results will be published under separate cover. During fieldwork, we performed the following tasks:

- Obtained background information including: Office of Management and Budget memorandum, National Institute of Standards and Technology publications, and prior GSA Office of Inspector General audit reports.
- Reviewed policies including GSA Order PBS 3490.1, "Document security for sensitive but unclassified paper and electronic building information," dated March 8, 2002.
- Interviewed PBS National and Regional officials to determine what controls they have in place to ensure the security of sensitive building information.
- Interviewed three government contractors to determine what controls they have in place to ensure the security of sensitive building information.
- Analyzed 28 projects, which included 43 contract files (15 Architect and Engineering (A/E), 21 prime contractors, and 7 lease construction contracts), to determine if appropriate language was included in the contract regarding the security of sensitive building information.
- Reviewed government and contractor files to ensure they are maintaining documentation that is required under PBS 3490.1.
- Analyzed the proposed revisions to PBS 3490.1 currently under development.

The audit work was conducted from November 2007 through May 2008. The audit was performed in accordance with generally accepted government auditing standards.

**AUDIT OF PBS'S CONTROLS OVER
SECURITY OF BUILDING INFORMATION
REPORT NUMBER A070216/P/R/R08005**

Results of Audit

The Public Buildings Service (PBS) needs to improve its implementation of controls over sensitive building information to reduce the risk of inappropriate disclosure of sensitive building information that may result in harm to people or property. PBS defined its security requirements for sensitive building data in General Services Administration (GSA) Order, PBS 3490.1 (PBS 3490.1) entitled, "Document security for sensitive but unclassified paper and electronic building information," which was issued in March 2002. Overall, implementation of the controls to meet the requirements for safeguarding sensitive building information varied widely. The oversight practices of PBS project managers and contracting officers to implement PBS security policies were inconsistent. The inconsistent implementation was especially evident in the contracts, as many contracts did not include the contractor's responsibility to use reasonable care to protect sensitive building information. While the majority of PBS staff interviewed was aware of PBS 3490.1, few had received formal training in the requirements and how to implement them. PBS is currently in the process of revising the security requirements in PBS 3490.1 and may be able to use this as an opportunity to address many of the issues identified by our review.

Controls over Security Requirements are not Consistently Applied Across the Regions

Implementation of security controls over sensitive building information is not consistently applied across GSA regions or projects. During our review, we examined 43 contract files to assess the implementation of PBS's Sensitive but Unclassified (SBU) information policy. In addition to evaluating contract files and documentation, we held discussions with the project managers and contracting officers to discern their knowledge and efforts to implement the security requirements for SBU building information.

We tested the contract files for compliance with the following six requirements from the PBS 3490.1:

Encryption of Electronic Media – Was electronic media being encrypted?

Notice of Disposal – Were disposal notices being collected from the contractors and placed in the official file?

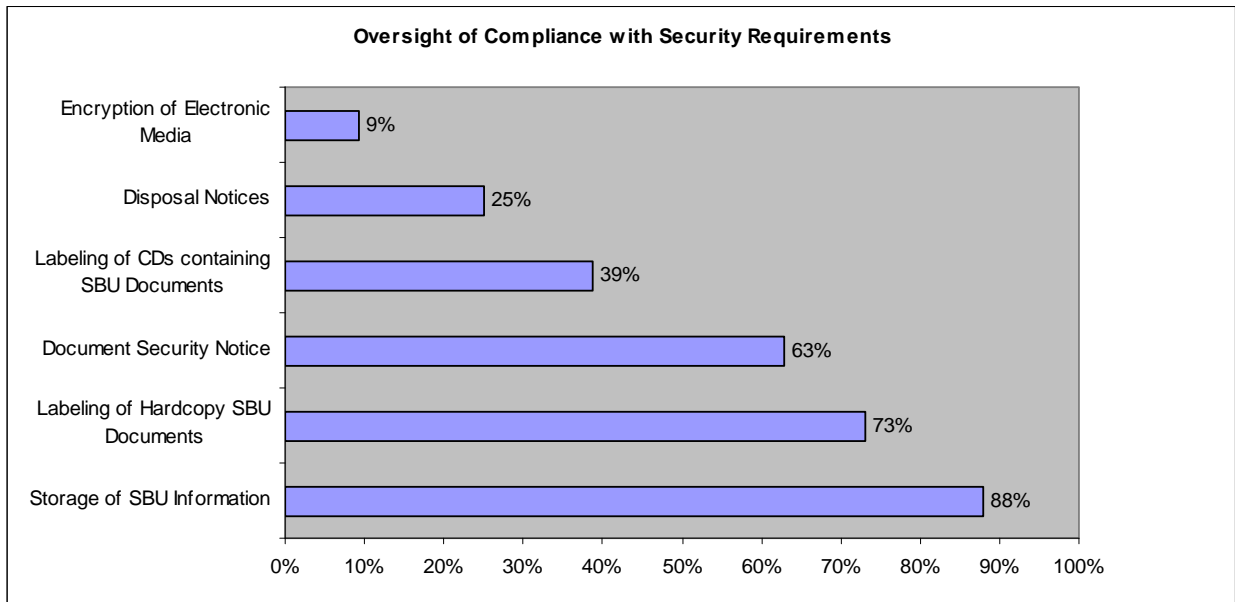
Labeling of Compact Disks (CDs) containing SBU Documents – Were CDs containing SBU documents properly labeled?

Document Security Notice – Were document security notices obtained from contractors and placed in the official file?

Labeling of Hardcopy SBU Documents – Were hardcopy documents containing SBU building information properly labeled?

Storage of SBU Information – Were SBU documents properly secured?

Of the six requirements, we found the least evidence for compliance with the requirement for Encryption of Electronic Media at 9 percent, while compliance with the requirement for the Storage of SBU Information was the most prevalent at 88 percent¹. The graph below indicates the frequency for each of the six requirements. As we stated above, oversight of security requirements was not consistently applied across the regions. Our analysis indicated that compliance by two of the regions was significantly higher than the third region. For example, Document Security Notices (DSN) were observed in two regions at 92 percent and 89 percent; however in the third region DSNs were only observed 15 percent of the time.



¹ We conducted our testing through interviews held with project managers and contracting officers, and performed physical observations when possible. When we were unable to conduct testing of the individual requirement for a contract, we excluded that contract from our sample analysis. Thus, for certain requirements, the total number of contracts reviewed may be less than 43.

Encryption of Electronic Media

When weighed against other contract oversight requirements, encryption of electronic media was the least followed requirement at a rate of 9 percent overall, with only 3 out of 32 contracts following the requirement. Encryption of Electronic Media is required by the PBS 3490.1 for the transfer and dissemination of sensitive information outside of the GSA intranet. In addition, the June 23, 2006 Office of Management and Budget Memorandum M-06-16 entitled “Protection of Sensitive Agency Information” recommends all departments and agencies encrypt all data on mobile computer/devices which carry agency data unless the data is determined to be non-sensitive.

The use of electronic media is common practice for both GSA and its contractors. It was common to use a CD to share sensitive information between GSA and parties whom GSA or a prime contractor determines have a legitimate need-to-know. Although CDs may be delivered to intended recipients by hand, other times delivery is performed using a bonded courier, which may increase the opportunity for a CD to be misplaced or delivered to an unintended party.

When we asked project managers and contracting officers throughout the Regions about unencrypted CDs in their possession, the most common responses given were (1) the Architect and Engineering (A/E) firm did not submit encrypted CDs to GSA, (2) the computers used by GSA lack encryption software and (3) the encryption process is time consuming. According to PBS Information Security Officials, PGP[®] encryption technologies have been made available to Regional personnel upon request, and according to the GSA Senior Agency Information Security Officer, WinZip 9.0[®], which supports 128 and 256 AES encryption, is installed in the standard GSA laptop configuration. Although GSA is not required by PBS 3490.1 to encrypt a CD if it is not intended for use outside of GSA, the possibility of the content of the CD being compromised by an unintended user is still present and the recommendation found in the M-06-16 should be followed.

Notice of Disposal

For contracts containing sensitive building information, the contractor is required by PBS 3490.1 to notify the GSA contracting officer that the contractor and its subcontractors have properly disposed of the information at the time of Release of Claims. We tested compliance with the Notice of Disposal requirement for 16 of the 43² contract files in our sample and found that four of the 16 (25 percent) of the contract files included some form of disposal notice. Many of the notices in the contract files were contractor generated e-mails or forms created by contracting officers for specific projects.

For proper disposal, hardcopy drawings are required by PBS 3490.1 to be burned or shredded. Many hardcopy drawings are too large to be destroyed by a conventional shredder; therefore, many contractors return the drawings to GSA, which may outsource the shredding.

² Many of the contracts we reviewed were in progress and were excluded from our testing of the disposal notice requirement.

Labeling CDs Containing SBU Documents

The PBS 3490.1 requires that sensitive building information in electronic format be labeled as follows:

**PROPERTY OF THE UNITED STATES GOVERNMENT
COPYING, DISSEMINATION, OR DISTRIBUTION OF THESE DRAWINGS, PLANS,
OR SPECIFICATIONS TO UNAUTHORIZED USERS IS PROHIBITED**

Do not remove this notice
Properly destroy documents when no longer needed

We verified the labeling of CDs containing SBU documents for 31 contracts and found that 12 contracts had CDs (39 percent) that were properly labeled. When we asked project managers and contracting officers about unlabeled CDs in their possession, the most common response was that A/E firms did not label the CDs before sending them to GSA. We did find that GSA had labeled many of the CDs themselves after they were received from the A/E firms; however, other recipients of unlabeled CDs may not correct the oversight.

Document Security Notice

PBS 3490.1 emphasizes that “dissemination of information shall only be made upon determination that the recipient is *authorized* to receive it.” Those who disseminate sensitive building information are required by PBS 3490.1 to obtain a signed Document Security Notice from the party to whom the information will be disseminated and maintain records of disseminated DSNs to be turned over to GSA at the completion of work. The DSN validates the identity of the recipient and assures that the recipient is authorized to receive the information. We tested compliance with the DSN requirement for 35 of the sample contracts and found that 22 (63 percent) of the contract files included DSN records³.

PBS 3490.1 “applies to all SBU building information regarding PBS controlled space or procurements to obtain PBS-controlled space, either government owned or leased... and includes GSA space that is delegated to other Federal agencies.” We were told by project managers and contracting officers for two of the projects without DSNs that GSA had adhered to the stricter document security protocol of the occupying agency and did not consider the DSN necessary. While certain circumstances may require adapting 3490.1, PBS needs to ensure that the intent of 3490.1 is met and all involved parties use reasonable care when handling SBU building documents.

³ Many of the projects we reviewed were in progress, thus they were excluded from our testing.

Labeling of Hardcopy SBU Documents

The PBS 3490.1 requires that each page of hardcopy drawings, excluding the cover, be labeled as follows:

**PROPERTY OF THE UNITED STATES GOVERNMENT
FOR OFFICIAL USE ONLY**

**Do not remove this notice
Properly destroy documents when no longer needed**

In addition, the PBS 3490.1 requires that the cover page of hardcopy drawings be labeled as follows:

**PROPERTY OF THE UNITED STATES GOVERNMENT
COPYING, DISSEMINATION, OR DISTRIBUTION OF THESE DRAWINGS, PLANS,
OR SPECIFICATIONS TO UNAUTHORIZED USERS IS PROHIBITED**

**Do not remove this notice
Properly destroy documents when no longer needed**

We tested compliance with the requirement for labeling hardcopy SBU drawings for 37 contracts. We found that 27 contracts (73 percent) had hardcopy drawings imprinted with the labeling above. While three other hardcopy drawings did contain property notice labels, they did not match the labels required by the PBS 3490.1. In two projects where drawings were not labeled, the project managers and contracting officers informed us that drawings had not been labeled because they did not identify building names, property locations or occupying agencies, so they thought they did not require SBU labels. However, the Labeling of Hardcopy SBU Documents requirement still applies to all hardcopy drawings that meet PBS 3490.1 criteria for determining information requiring document security.

Storage of SBU Information

Of the six requirements included in our oversight analysis, the Storage of SBU Information requirement was followed most. We reviewed the Storage of SBU Information for 33 contracts. Of the 33 contracts, we found that the Storage of SBU Information requirement was followed for 29 contracts (88 percent.)

It is common for GSA contractors to have on-site plan rooms in which sensitive building information is available to employees and subcontractors. We visited two on-site contractor facilities that contained sensitive building information and observed that the facilities were equipped with security devices such as monitoring alarm systems and exterior fencing. We also visited GSA facilities and verified that GSA was maintaining sensitive building information in secured PBS space when the information was in use and when the information was no longer needed. PBS 3490.1 requires that unneeded sensitive building information be destroyed; however, GSA, the A/E firm, and the general contractor are allowed to keep necessary record copies. Those record copies are required by PBS 3490.1 to be properly safeguarded throughout the retention period. In GSA, such copies were stored in restricted access space.

PBS Security Requirements are Often not Included in Construction Contracts

The results of the contract file review indicate that the security requirements for sensitive building data are not being performed consistently. The inconsistent implementation was especially evident in the contracts themselves, as many contracts did not include language that would obligate contractors to use reasonable care to protect sensitive building information. We analyzed the contracts to determine whether they included the following requirements of PBS 3490.1:

Reference to PBS 3490.1 – Did the contract directly reference PBS 3490.1 in its entirety?

Inclusion of Encryption Requirements – Did the contract require that the transfer and dissemination of SBU information beyond the GSA Intranet be encrypted?

Labeling of SBU Documents – Did the contract require the proper labeling of electronic and paper SBU documents?

Storage of SBU Information – Did the contract require the proper storage of SBU building information to be safeguarded during use?

Inclusion of Data Ownership – Did the contract specify that all drawings shall become the property of the United States Government?

Document Security Notice – Did the contract require those disseminating SBU building information to obtain a signed copy of a Document Security Notice from the recipient of SBU documentation?

Notice of Disposal – Did the contract require the contractor to submit a Notice of Disposal at the time of the Release of Claims?

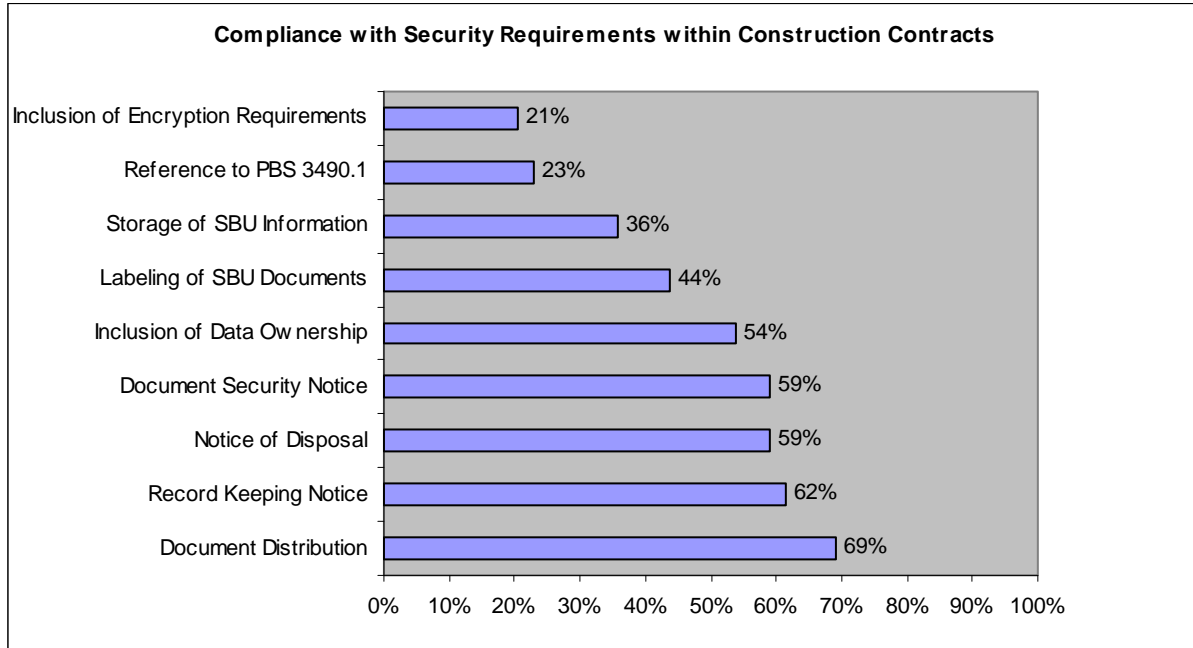
Record Keeping Notice – Did the contract require the disseminator of SBU building information to keep records of Document Security Notices and provide those records to GSA to be kept with the permanent contract file?

Document Distribution – Did the contract require the disseminator to limit distribution of SBU building information to those with a need-to-know?

During our analysis of 43 contract files, we found that direct references to GSA's security policy PBS 3490.1 or inclusion of its requirements are often lacking in GSA construction contracts. Only 23 percent of the files reviewed included a copy or a direct reference to PBS 3490.1 requirements. Although some of the contracts in our sample contained clauses requiring the contractor to adhere to the PBS Computer Aided Design (CAD) Standards and the Facilities Standards for the Public Buildings Service PBS P-100 whose recent versions reference PBS 3490.1, the contractor's knowledge of this obligation to comply with the PBS 3490.1

requirements would be predicated on noticing an isolated reference in a multi-page document and then locating a copy of PBS 3490.1.

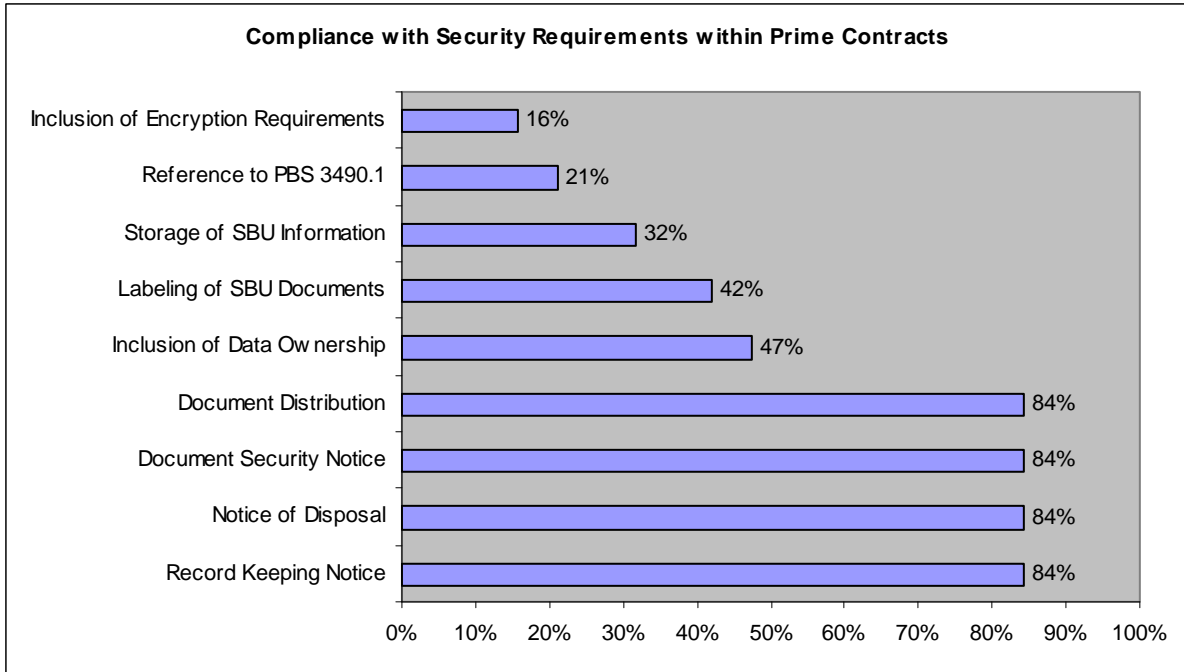
The full results of our analysis to determine whether or not the contract files referenced GSA's security policy PBS 3490.1 or its requirements are summarized in the following chart.



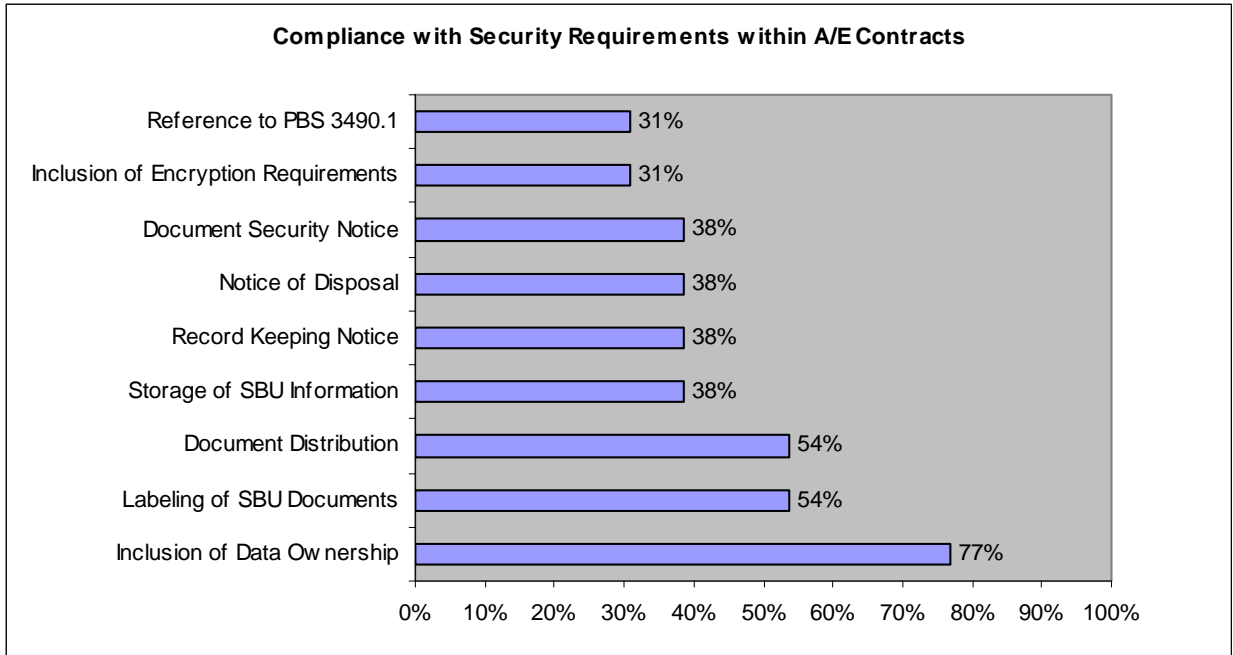
The summary shows that of the nine references tested, we found that the encryption requirement was included in contracts least often at a rate of 21 percent and that document distribution was included most often at a rate of 69 percent.

Inclusion of Security Requirements Varied Between Contract Types

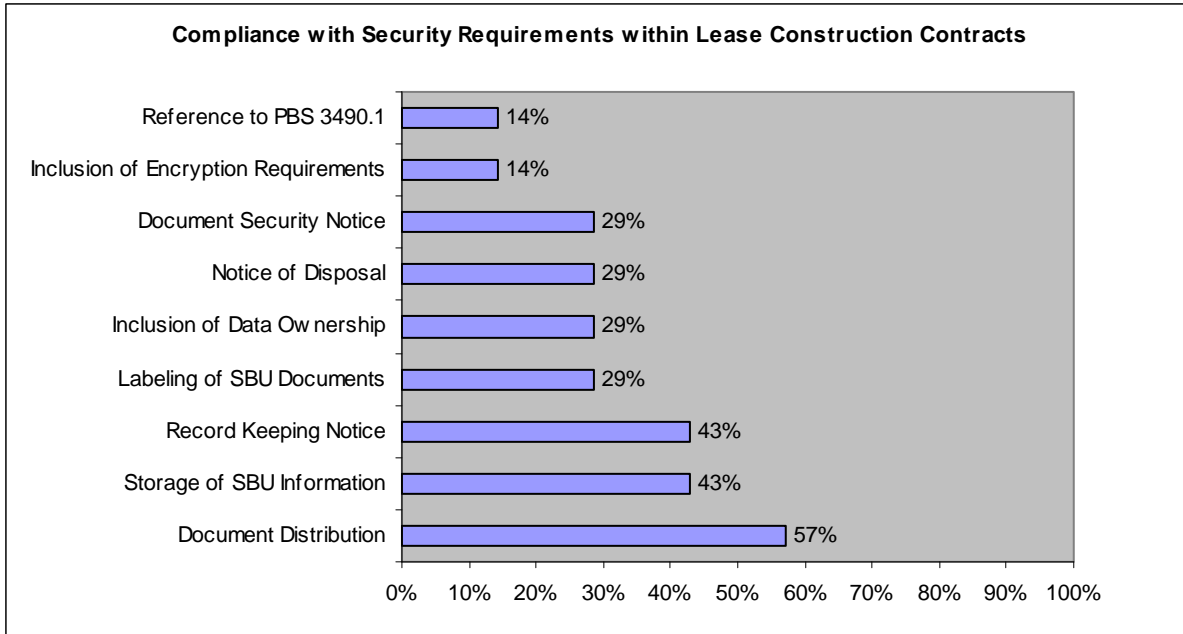
The inclusion of GSA security requirements in A/E, prime, and lease construction contracts varied widely. As depicted in the following graphs, prime contracts showed the highest level of security requirements, followed by A/E contracts. Lease construction contracts included the least requirements.



Document Security Notices were included in prime contracts 84 percent of the time. Many Regions followed a best practice of including a copy of a DSN within the contract and required prime contractors to complete this form before receiving copies of SBU information. The DSN is an attachment to the PBS 3490.1 that serves as an agreement by the contractor that they will only disseminate SBU building information to other authorized users under the conditions set forth within the notice. Although the DSN includes three other requirements of the PBS 3490.1 (document distribution, notice of disposal, and record keeping notice), the DSN doesn't encompass all the PBS 3490.1 requirements. For those requirements that were not included in the DSN, inclusion into the contracts was significantly less, as shown above. Although prime contracts usually included DSNs, all requirements need to be included in the contract to hold the contractor responsible for properly protecting SBU building information in their possession.



Three requirements were included in A/E contracts more than half the time: document distribution and labeling of SBU documents at 54 percent, and data ownership at 77 percent. Six other requirements, as noted above, were included in A/E contracts 38 percent of the time or less. These results may be affected by some of the A/E contracts in our sample being awarded shortly after the implementation of PBS 3490.1. In fact, two of the A/E contracts we reviewed were Indefinite Delivery Indefinite Quantity (IDIQ) contracts that were awarded before the issuance of PBS 3490.1. However, the purchase of A/E services off these IDIQ contracts was made after the issuance of PBS 3490.1. Accordingly, we analyzed all task orders, contract amendments and modifications and none were modified to include GSA SBU document security requirements after the issuance of PBS 3490.1. To properly secure SBU building information, it is imperative that the proper GSA security requirements are placed in A/E contracts.



Document distribution is included in lease construction contracts 57 percent of the time. Although the overall percentages are low, lease construction includes obstacles not found in other contracts. In lease construction, the lessor contracts with its own A/E and prime contractors. Thus, the contracting officer cannot directly negotiate GSA security requirements into the A/E and prime contracts. In one project, PBS realty officials requested a proposal from the lessor to implement the PBS 3490.1 requirements. In response, the lessor proposed a price of \$100,000. The tenant agency was unwilling to absorb this amount and requested reduced SBU document security requirements. To ensure GSA document security requirements are included in the lease, PBS should place its requirements into its boilerplate lease contract language. A clause should also be included in the boilerplate lease that requires the lessor to include GSA security policies in its A/E and prime contracts. Inclusion of GSA security policies into the boilerplate lease should eliminate the need to negotiate potentially costly supplemental lease agreements for the implementation of GSA security requirements.

Contractors Adhered to Security Requirements

We performed site visits to two prime contractor locations, and held a teleconference with a third. Two were familiar with the requirements of PBS 3490.1, and all noted that PBS representatives had conveyed the importance of safeguarding SBU building documents. During our site visits, we verified that the contractors were maintaining SBU dissemination records, including obtaining DSNs from subcontractors, and were making efforts to obtain disposal notices, where applicable. We also observed that SBU documents were stored in secure locations.

Since one of the aims of PBS's SBU policy is to protect sensitive building information, without restrictive requirements which might hamper competition, we obtained the contractors' insights on how burdensome the current SBU requirements were and how costly it was for the

contractors to meet them. None of the contractor's considered the SBU requirements, by themselves, to be particularly burdensome or costly to fulfill. A similar query was made of the contracting officers and project managers we met with during this review. Their responses mirrored the contractors. Most had never received complaints specifically about the SBU requirements. However, as discussed previously, one lessor believed the 3490.1 requirements so burdensome he wanted \$100,000 to implement them.

Contracts Should Include Requirements for Safeguarding Sensitive Building Information

The primary non-government users of SBU building information are the contractors that perform the construction related work required by PBS. This is true for A/E and prime contractors on construction contracts as well as lessors for lease construction contracts. It is imperative that these contractors have an understanding of PBS's expectations for safeguarding sensitive building information so they can use reasonable care when handling applicable SBU documents. As such, GSA should include the contractors' responsibilities for safeguarding sensitive building information in the contract. This should include requirements that contractors and lessors should inform their subcontractors working on GSA constructions projects of the requirements and responsibilities for safeguarding sensitive building information. PBS should also use contractual language to establish penalties for noncompliance. Currently, there are no statutory penalties for failing to properly safeguard SBU building information. If a security breach does occur and these security requirements are not included in the contract, GSA's ability to take action against the negligent party will be limited.

Formal Training for the Project Team is Needed

During our review we found that the majority of PBS project managers and contracting officers were aware of the PBS 3490.1; however, few had received training outlining the requirements or procedures. PBS 3490.1 requires that Federal Government employees who handle sensitive building information have security training in which the PBS 3490.1 and its procedures are outlined. When asked about training as it relates to PBS 3490.1, several project managers and contracting officers replied that they had attended meetings in which the PBS 3490.1 was discussed by upper management. However, the majority replied that they had received the PBS 3490.1 via e-mail and had not received any form of training on the document. Security training, as required by the PBS 3490.1, will consistently educate the project team on actions to reduce the risk that sensitive building information will be used for dangerous or illegal purposes. Such training should be included in the annual training plan for PBS employees who handle sensitive building information.

PBS is Currently Drafting Revisions to GSA Order, PBS 3490.1

PBS has established a team to revise PBS 3490.1 to “provide updated guidance to reflect changes issued by, among others, the White House memorandum, dated May 9, 2008, the National Institute of Standards and Technology, and federal acquisition policies”. The President of the United States memorandum dated May 9, 2008 entitled “Designation and Sharing of Controlled Unclassified Information,” adopts, defines, and institutes "*Controlled Unclassified Information*" (CUI) as the single, categorical designation henceforth throughout the executive branch for all information within the scope of that definition. This includes most information referred to as "*Sensitive But Unclassified*" (SBU) in the Information Sharing Environment” and “establishes a corresponding new CUI Framework for designating, marking, safeguarding, and disseminating information designated as CUI.” The memorandum establishes three new designations: (1) "Controlled with Standard Dissemination; (2) Controlled with Specified Dissemination; and (3) Controlled Enhanced with Specified Dissemination", depending upon the safeguarding procedures and dissemination controls deemed necessary. The PBS revision team consulted with the GSA Office of General Counsel and the National Archives and Records Administration regarding the impact of the new requirements on PBS SBU protection policies. The team was advised that the proposed revisions contain the correct terminology.

Conclusion

PBS needs to improve its implementation of controls over sensitive building information to reduce the risk of inappropriate disclosure of sensitive building information that may result in harm to people or property. Although PBS is revising its current policies with regard to document security for sensitive but unclassified paper and electronic building information, it also must make certain that proper controls are in place to ensure its policies, old or new, are enforced. As our findings indicate, the implementation of PBS 3490.1 security requirements has been inconsistent and needs management oversight. Project files and discussions with team members indicate inconsistent implementation of requirements, inclusion of contractor responsibilities varies by contract, and formal training of GSA personnel on its security policies is also needed. Also, during our discussions with PBS personnel and the review of documentation, we did not encounter indications that implementation of PBS 3490.1 security requirements were being verified by any PBS internal control review group. Given these issues, PBS needs to establish a system to ensure that its requirements for safeguarding sensitive building information are implemented consistently on all projects.

Recommendations

We recommend that the PBS Commissioner:

1. Incorporate PBS 3490.1 requirements directly into the boilerplate Solicitation for Offers and contracts for A/Es, construction, and lease construction contracts.
 - a. Require contractors to include PBS 3490.1 requirements in their subcontracts.
 - b. Develop a course of action to be taken when contractors do not fulfill their contractual obligations regarding the protection of SBU information.
2. Ensure PBS officials are provided training on the PBS 3490.1. The training should include encryption software applications available to PBS project personnel.
3. Implement a system of controls to ensure that PBS 3490.1 requirements are being followed by PBS project teams.

Management Comments

PBS believes the report's objectives are valid and accepted its three recommendations.

Management Controls

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

Appendices

**AUDIT OF PBS'S CONTROLS OVER
SECURITY OF BUILDING INFORMATION
REPORT NUMBER A070216/P/R/R08005**

Appendix A

Management Response



U.S. General Services Administration

SEP 29 2008

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

FROM: DAVID L. WINSTEAD
COMMISSIONER (P)

A handwritten signature in black ink, appearing to read "D. Winstead", written over the printed name of David L. Winstead.

SUBJECT: Draft Report: Audit of PBS's Controls Over Security of Building
Information (Report Number A070216) dated August 27, 2008

Thank you for the opportunity to review and comment on the subject draft audit report. PBS believes the report's objectives are valid and we accept its three recommendations as follows:

1. Incorporate GSA Order PBS 3490.1 requirements directly into the boilerplate Solicitation for Offers and contracts for A/Es, construction, and lease construction contracts.
 - a. Require contractors to include PBS 3490.1 requirements in their subcontracts.
 - b. Develop a course of action to be taken when contractors do not fulfill their contractual obligations regarding the protection of Sensitive but Unclassified (SBU) information.
2. Ensure PBS officials are provided training on PBS 3490.1.

The training should include encryption software applications available to PBS project personnel.
3. Implement a system of controls to ensure that PBS 3490.1 requirements are being followed by PBS project teams.

We will develop a Corrective Action Plan to address these recommendations.

1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

**AUDIT OF PBS'S CONTROLS OVER
SECURITY OF BUILDING INFORMATION
REPORT NUMBER A070216/P/R/R08005**

Appendix B

Report Distribution

	<u>Copies</u>
Commissioner, Public Buildings Service (P)	3
Regional Administrator, National Capital Region (NCR)	1
Regional Administrator, Southeast Sunbelt Region (4A)	1
Regional Administrator, Greater Southwest Region (7A)	1
Regional Inspector General for Auditing (NCR, JA-4, JA-7)	3
Regional Inspector General for Investigation (JI-W, JI-4, JI-7)	3
Office of Inspector General (J)	4
Assistant Inspector General for Auditing (JA, JAO)	2
Assistant Inspector General for Investigation (JI)	1
Office of the Chief Financial Officer (B)	1
Director, Internal Control & Audit Division (BEI)	1