



Office of Audits
Office of Inspector General
U.S. General Services Administration

Audit of IT Security Requirements in GSA Leasing Support Services Contracts

Report Number A170092/P/R/R19004
March 21, 2019

Executive Summary

Audit of IT Security Requirements in GSA Leasing Support Services Contracts

Report Number A170092/P/R/R19004

March 21, 2019

Why We Performed This Audit

We performed this audit in response to a hotline complaint regarding GSA's efforts to assist the GSA Leasing Support Services (GLS) contractors in meeting the contracts' information technology (IT) security requirements. Our objective was to determine if GSA's award and administration of the GLS contracts sufficiently protected government data. In particular, we focused on GSA's changes to the IT security requirements for the GLS contracts.

What We Found

GSA did not effectively manage changes to the IT security requirements for the GLS contracts. We found that GSA's administration of the GLS contracts resulted in a violation of federal competition requirements. GSA significantly changed the contractors' IT security obligations subsequent to contract award. By materially altering the time and cost associated with meeting the contracts' IT security requirements, GSA made a cardinal change to the contracts and violated the Competition in Contracting Act and the Federal Acquisition Regulation.

Additionally, we found that GSA lacked assurance that government data maintained on contractor systems was secure because GSA did not issue contract modifications or guidance reflecting the changes to the GLS contracts' IT security requirements for more than 1 year after the changes were made. This led to a substantial period in which the contracts' IT security requirements were unclear and government data stored on contractor systems was potentially vulnerable to misuse.

What We Recommend

We recommend that the Commissioner, Public Buildings Service:

1. Coordinate with GSA IT to ensure that the IT requirements and solutions for the pending GLS Plus real estate broker solicitation accurately reflect the actual IT security requirements for contractor performance.
2. Identify other Public Buildings Service contracts through which contractors access government data through GSA Google or Virtual Desktop Interface accounts to ensure:
 - a. The contracts include terms and conditions necessary to protect the data; and
 - b. Guidance is in place defining roles and responsibilities governing compliance with applicable IT security requirements.

In his response, the Commissioner of the Public Buildings Service agreed with our recommendations. The Commissioner's written comments are included in their entirety as ***Appendix B***.

Table of Contents

Introduction	1
Results	
<i>Finding 1 – GSA significantly changed the GLS contractors’ IT security obligations subsequent to award, resulting in a cardinal change to the contracts that violated federal competition requirements.....</i>	<i>3</i>
<i>Finding 2 – GSA did not have assurance that government data maintained on contractor systems was secure because it did not issue GLS contract modifications or guidance that reflected changes to the contracts’ IT security obligations in a timely manner.. ..</i>	<i>8</i>
Conclusion.....	11
<i>Recommendations</i>	<i>11</i>
<i>GSA Comments.....</i>	<i>11</i>
Appendixes	
Appendix A – Scope and Methodology.....	A-1
Appendix B – GSA Comments	B-1
Appendix C – Report Distribution	C-1

Introduction

We performed an audit of GSA's contracting actions related to changes in the information technology (IT) security requirements in the GSA Leasing Support Services (GLS) contracts.

Purpose

We performed this audit in response to a hotline complaint regarding GSA's efforts to assist the GLS contractors in meeting the contracts' IT security requirements.

Objective

Our objective was to determine if GSA's award and administration of the GLS contracts sufficiently protected government data. In particular, we focused on GSA's changes to the IT security requirements for the GLS contracts.

See **Appendix A** – Scope and Methodology for additional details.

Background

As part of its mission to provide effective workplace solutions for federal agencies at best value, GSA's Public Buildings Service (PBS) leases space from the private sector to meet customer needs. Approximately half of the federal workforce is housed in leased space. Since 2005, PBS has contracted for broker services to help manage its extensive lease acquisition workload. As of September 30, 2017, PBS had 187.6 million rentable square feet under lease nationwide, with a total annual rental of space expense of \$5.5 billion.

The national broker contracts provide leasing support services, such as market surveys, site visits, document preparation, and lease negotiations. The national broker contracts are "no-cost" contracts; contractors collect real estate commissions paid by the building owner in lieu of direct payment by GSA for services performed. While the brokers have a significant role in PBS's lease acquisitions, PBS personnel are required to oversee the brokers' work and complete inherently governmental tasks related to lease award and administration, such as signing a lease and determining fair and reasonable pricing.

The GLS contracts are GSA's third generation of the national broker contracts. The PBS Office of Leasing's Center for Broker Services is responsible for the award and administration of these contracts. The Center for Broker Services awarded the GLS contracts in September 2015, with a Notice to Proceed issued in January 2016. The initial awards included a 1-year base period, with four 1-year option periods. If PBS exercises all option periods, the contracts will expire in January 2021.

GSA awarded nine GLS contracts to six brokers. The contracts were divided into four geographic zones in order to encourage small business participation. Four of the GLS contractors are incumbents who had prior national broker contracts with GSA; two GLS contractors were new small business awardees.

In May 2017, we received a hotline complaint alleging that GSA changed the IT security requirements of the GLS contracts without issuing corresponding contract modifications. The GLS contracts have extensive IT security requirements to protect the federal information and computer systems accessed by the brokers. These systems include sensitive government information such as market surveys with rental rates and information about the federal tenants. The information about federal tenants includes security needs and floorplans.

Under the terms of the GLS contracts, brokers are subject to all GSA and federal IT security standards, policies, and reporting requirements. The GLS contracts incorporate by reference the GSA Information Technology Security Policy (GSA Order CIO P 2100.1), the Federal Information Security Management Act (FISMA) of 2002, and the Federal Information Processing Standards. GSA IT, formerly known as the Office of the Chief Information Officer, manages the IT security program for GSA and acts as the Information System Security Manager for the GLS contracts, ensuring compliance with the GLS contracts' IT security requirements. Accordingly, GSA IT is responsible for authorizing the contractors' systems to access GSA data and monitoring the submission of the contractors' IT security deliverables.

Results

GSA did not effectively manage changes to the IT security requirements for the GLS contracts. We found that GSA's administration of the GLS contracts resulted in a violation of federal competition requirements. GSA significantly changed the contractors' IT security obligations subsequent to contract award. By materially altering the time and cost associated with meeting the contracts' IT security requirements, GSA made a cardinal change to the contracts and violated the Competition in Contracting Act and the Federal Acquisition Regulation (FAR).

Additionally, GSA lacked assurance that government data maintained on contractor systems was secure because GSA did not issue contract modifications or guidance reflecting the changes to the GLS contracts' IT security requirements for more than 1 year after the changes were made. This led to a substantial period in which the contracts' IT security requirements were unclear and government data stored on contractor systems was potentially vulnerable to improper use.

Finding 1 – GSA significantly changed the GLS contractors' IT security obligations subsequent to award, resulting in a cardinal change to the contracts that violated federal competition requirements.

The Competition in Contracting Act of 1984 (41 U.S. Code 3301) and FAR 6.101(a) require "full and open competition" using competitive procedures in government procurements unless otherwise authorized by law. After a contract is competitively awarded, the contract cannot be so materially altered by negotiation between the contractor and the government as to constitute a cardinal change to the contract.

GSA violated these requirements by significantly altering the IT security obligations of the GLS contracts after award. Under GSA's original solicitation for the GLS contracts, bidders were required to have IT systems that complied with costly IT security requirements to access leasing information through GSA systems. GSA used these IT security requirements as a basis for evaluating offers, in one instance rejecting an offer because the bidder did not demonstrate that its systems could comply with the requirements. However, subsequent to award of the GLS contracts, GSA offered contractors the option to use GSA-managed systems to access and store the leasing data. In doing so, GSA materially transferred many of the contractors' IT security obligations to GSA, and substantially reduced the contractors' costs. This change likely altered the scope of competition for the GLS contracts and thereby constituted a cardinal change that did not comply with federal competition requirements.

GSA's violation of the competition requirements is discussed below.

GSA's Solicitation and Pre-Proposal Questions and Answers Detail Extensive IT Requirements

On April 20, 2015, the Center for Broker Services issued its final solicitation for GLS services. The solicitation required contractors to have access to the GSA Real Estate Exchange (G-REX) system, a lease acquisition program tool, from their computer systems to perform their contract duties. Under Section H of the solicitation, contractors were required to comply with a number of IT security requirements in order to gain access to G-REX. Among other things, contractors were required to conform with:

- All GSA and federal IT security standards, policies, and reporting requirements; and
- General Services Acquisition Regulation provisions that establish contractors' responsibilities for IT security for all contractor-maintained systems connected to a GSA network.¹

In the Pre-Proposal Questions and Answers for the final solicitation, GSA emphasized the importance of compliance with these requirements before GSA issued the Notice to Proceed:

11. Given the new additional vendor requirements under FISMA, will you allow a reasonable timeframe (for example, 18 months) to comply with the new requirements?

Response: No, the successful offeror must be FISMA compliant before GSA can issue the notice to proceed (NTP). NTP is anticipated to be issued on [or] around February 4, 2016.

To ensure compliance with the contract's IT requirements prior to the issuance of the NTP, GSA was to review each contractor's system through a formal approval process known as the Assessment and Authorization. If GSA determined that the contractor's system was compliant, it was required to issue an Authority to Operate before the contractor could operate and process GSA information on its system.² Throughout the life of the contract, each GLS contractor had to submit a number of IT security deliverables to GSA to allow monitoring of its IT security compliance. For example, GLS contractors were to provide incident response test reports to GSA, for GSA's use in determining whether the contractors were appropriately responding to IT system breaches.

¹ General Services Acquisition Regulation 552.239-70, *Information Technology Security Plan and Security Authorization* and 552.239-71, *Security Requirements for Unclassified Information Technology Resources*.

² An Authority to Operate is valid for 3 years.

GSA Provides GSA Google Accounts to Contractors Having Difficulty Meeting IT Requirements

During the 3.5 months between contract award and the planned NTP, GSA IT determined that the two small business contractors did not have sufficient time to develop IT systems that would meet FISMA requirements before the planned NTP. Unlike the IT systems of the four large business contractors that possessed prior experience as GSA real estate brokers, these two small business contractors' IT systems were not previously assessed and authorized by GSA. As a temporary fix for the small business contractors that were having difficulty meeting the contracts' significant IT requirements, GSA provided these contractors with GSA Google accounts for file storage in January 2016.

This initial alteration of the contract requirements was driven by PBS's perceived need to issue the NTP to avoid a lapse in services. The acquisition plan for the GLS contracts states:

The need for a follow on contract in place, prior to the expiration of the current contract is significantly driving this requirement, due to the current time constraints. The schedule goal of awarding contracts and issuing the Notice to Proceed ... is the most important goal.

In explaining the temporary fix for the small business contractors, the Center for Broker Services Director noted in an email to the contracting personnel, "[t]he only other option is to delay issuing the NTP and I am not sure that is going to be acceptable."

By August 2017, GSA had modified the contracts for all six of the GLS contractors (discussed further in *Finding 2*) to require the use of GSA Google email accounts for all email correspondence relating to performance of the contract. As of July 2018, GSA had provided 116 GSA Google accounts to the six GLS contractors.

GSA Provides Virtual Desktop Interface Accounts to Reduce Costs and Increase Security

After PBS awarded the contracts, GSA IT recommended the use of GSA Virtual Desktop Interface (VDI) accounts, which can be used in conjunction with GSA Google accounts, as a means of reducing compliance costs and increasing IT security. These accounts allow brokers to access GSA's systems through the GSA network, as opposed to the contractors' servers. The contracting officer's representatives described the rationale behind this recommendation in a memorandum to the contracting officers dated June 12, 2017:

In November 2015, GSA-IT Security managers ... approached the Center for Broker Services (PRAA) with a proposal to simplify FISMA security requirements and reduce GSA's compliance costs. With [the] IT Security team, PRAA researched the viability of utilizing a Virtual Desktop Interface (VDI) over a series of meetings with [the Office of] General Counsel We concluded that moving to VDI would provide the highest security compliance for broker contracts, allow the fewest vulnerabilities and reduce costs for compliance and oversight.

Of the six GLS contractors, five chose to transition to the VDI accounts. In August 2016, GSA began the process to transition the first contractor to VDI. In October 2016, GSA provided that contractor with VDI accounts. In February 2017, GSA provided VDI accounts to four additional GLS contractors. By August 2017, GSA modified the contracts (discussed further in *Finding 2*) to require the contractors that transitioned to VDI to use it to access all GSA IT resources necessary to work under the contract, including VDI file servers, Google Drive, G-REX, and GSA Google email. As of August 2018, GSA had provided 89 active VDI accounts to GLS contractors.³

Changes in Performance Costs and Effort with GSA Google and VDI Accounts

In providing GSA Google and VDI accounts to GLS contractors, PBS significantly changed the GLS requirements from the solicitation in two key areas – performance costs and level of effort.

Performance Costs. In its acquisition plan, PBS acknowledged the significant start-up costs associated with the contracts’ IT security requirements, estimating the administrative start-up costs ranged from \$500,000 to \$1 million. These costs were due in part to the FISMA requirements, including the costs of IT training and dedicated IT servers needed to access G-REX, and in part to non-FISMA firewall requirements to address potential conflicts of interest.⁴ A contracting officer’s representative estimated that using VDI accounts would result in total cost savings for contractors at upwards of \$1 million over the life of the contract.

Level of Effort. The solicitation states that the IT security requirements in Section H are “significant” and provides that contractors will have to expend “time and effort to comply” with those requirements. However, when GSA changed the contract requirements by offering contractors use of GSA Google and VDI accounts, contractors no longer had to develop or use their own FISMA-compliant systems to access GSA systems or take any steps to comply with the following GLS contract requirements:

- 19 of the 25 policies and regulations listed in the original contract;
- All of the contract requirements in Section H.3.4.2, *GSA Security Compliance Requirements*, and Section H.3.4.3, *Assessment and Authorization (A&A) Activities*;
- 16 of the 17 contract quarterly and annual deliverables required under Section H.3.4.4, *Reporting and Continuous Monitoring*; and
- 3 of the 5 contract requirements in Section H.3.4.5, *Additional Stipulations*.

³To access their VDI accounts, GLS contractors use a two-factor authentication process. In addition to their username and password (first factor), a code will be sent to their mobile device (second factor). GSA monitors the GLS contractors’ accounts in the same way it monitors GSA employee accounts. Specifically, GSA disables accounts if a user is inactive for 120 days or if the user does not complete annual mandatory training.

⁴The firewall requirements are intended to avoid, neutralize, or otherwise mitigate organizational conflicts of interest that might exist related to contractors’ performance of work required by the GLS contracts. Such conflicts may exist if a contractor represents an offeror for a GLS task order. None of the contractor’s personnel may participate as both a GSA representative and as a representative of an offeror.

Effects on Competition

Given that the change in requirements significantly reduced both IT security compliance costs and performance obligations, GSA could have eliminated a barrier to entry by providing an option to use GSA-provided IT systems in the solicitation. Such an option would have made it feasible for more companies, including small businesses and those with no or limited experience in meeting federal FISMA requirements, to make a competitive offer. While more than 40 companies attended the two pre-proposal conferences conducted for this procurement, only 12 companies ultimately submitted an offer.

In addition to limiting the scope of competition, GSA assessed contractors' IT proposals using the more stringent IT requirements set forth in the solicitation. In the technical factor review of GSA's source selection, at least one offeror's system was assessed as being at risk of not meeting these requirements. The source selection board evaluated an offeror's technology to access G-REX as a risk and GSA did not award this contractor a GLS contract.

Subsequent to contract award, GSA made a cardinal change to the GLS contracts by significantly relaxing the contracts' IT security requirements, which were an essential element of the contracts and part of the award evaluation. As a result, GSA likely altered the scope of competition because contractors who were capable of performing the work at a potentially lower cost were not provided the opportunity to compete for the work.

A PBS contracting officer told us that the change to allow the use of GSA Google and VDI was not significant because the underlying IT security requirements of the GLS contracts remained the same. The contracting officer asserted that the use of GSA Google and VDI were simply a means to meet these requirements. However, this is incorrect.

The GLS contracts required contractors to use their own systems to access GSA data and required that the contractors' systems meet various IT security requirements. As noted above, this was a significant contract requirement and served as a factor in GSA's evaluation of offerors' proposals. GSA's introduction of the Google and VDI options to access GSA data meant that contractors no longer had to use their own systems to access this data. Therefore, GSA had more control and assurance over the contractors' access and maintenance of Agency data and was able to significantly relax the contracts' IT security requirements accordingly. In doing so, GSA substantially altered the contracts' IT security requirements after award resulting in a cardinal change.

PBS should coordinate in depth with GSA IT regarding IT requirements and solutions for the pending GLS Plus real estate broker solicitation.

Finding 2 – GSA did not have assurance that government data maintained on contractor systems was secure because it did not issue GLS contract modifications or guidance that reflected changes to the contracts’ IT security obligations in a timely manner.

Although GSA made significant changes to the GLS contracts’ IT security requirements, it did not issue contract modifications memorializing the revised requirements or guidance outlining roles and responsibilities surrounding the new requirements for more than 1 year after the changes were made. As detailed below, this led to an extended period in which requirements necessary to protect government data were lacking. Therefore, GSA lacked assurance that this data was secure.

Lack of Contract Modifications Led to Uncertainty About IT Security Requirements

According to FAR 43.103(a)(3), contract modifications are used to reflect agreements of the contracting officer and contractor modifying the terms of the contracts. However, at the time that GSA provided GSA Google and VDI accounts to the GLS contractors, thereby substantially altering the contracts’ IT security requirements, the contracting officers did not issue modifications as required. This caused confusion surrounding the contracts’ IT security requirements, which affected contractor performance and potentially exposed government data to risk.

GSA provided two contractors with GSA Google accounts in January 2016 and provided five contractors with VDI accounts in August 2016 and February 2017. Although these actions resulted in significant changes to the IT security obligations for these contractors, GSA did not modify the contracts to reflect these changes until July and August 2017 – after we asked for the related modifications.⁵ Absent properly executed contract modifications, GSA and contractors should have followed the original terms and conditions stated in the GLS contracts. However, the discrepancy between GSA’s informal direction to the contractors about the use of GSA Google and VDI accounts and the original contract requirements created uncertainty and confusion about the contracts’ requirements, which affected contractor performance.

For example, after receiving a GSA Google account, one contractor continued to use its private servers to store GSA data for a period of 9 months. However, GSA had not authorized the contractor’s private servers for this purpose in accordance with the contract’s IT security requirements. Accordingly, in February 2017, GSA issued a cure notice to the contractor for its use of the noncompliant servers. The contractor accepted responsibility and stated in response, “My perception of the move to VDI meant that Google drive would not be utilized and we were to proceed as normal (with the company shared drive) until the transfer to VDI.”

⁵ Two of the nine GLS contracts were modified on July 13, 2017. The remaining seven GLS contracts were modified on August 8, 2017.

Additionally, although the four large business contractors continued to use their own IT systems between June and September 2016 in anticipation of receiving GSA Google and VDI accounts, these contractors did not submit 32 of the 60 required IT security deliverables designed to protect the government data accessed and stored by the contractors.⁶ These included major IT deliverables, such as:

- System security plans – These plans detail internal controls for the contractors’ IT systems;
- Incident response test reports – These reports are used to determine if the contractors are appropriately responding to IT system breaches; and
- Configuration management plans – These plans detail processes on how the contractors manage and monitor changes to their IT systems to ensure data is stored and accessed securely.

GSA monitored the missing deliverables during these quarters and noted the cause as “[contractor] is moving to the VDI solution in the near term and will be decommissioning its FISMA system.” However, by not enforcing the requirement for contractors to submit these IT deliverables, GSA placed government data at risk. Until the contractors’ transition to GSA Google and VDI was complete, GSA officials should have administered the terms and conditions of the original contract. Though GSA has since modified the GLS contract, it should identify other contracts through which the contractors access government data through GSA Google and VDI accounts to ensure the contracts include the terms and conditions necessary to protect the data.

Lack of Guidance Defining Roles and Responsibilities

GSA also did not issue guidance governing IT security roles and responsibilities under the GLS contracts for more than 1 year after it initiated the transition to the use of GSA Google and VDI accounts. In August 2017, GSA issued the *GLS National Quality Control Plan for IT Security* governing the contractors’ use of GSA Google and VDI. GSA provided that “the intent of this plan is to delineate roles and responsibilities and establish procedures to ensure contractors are compliant with IT Security Requirements...” and to “[e]nsure sufficient controls are in place to protect Government data.” However, the delay in issuing this guidance led to a significant period in which these requirements were not defined, thereby limiting GSA’s assurance that the government data was secure.

⁶ GSA IT stated that the two small business contractors did not need to submit deliverables to meet the contract requirements because the GSA Google accounts had already been assessed and granted an Authority to Operate.

Specifically, until the plan was issued, GSA did not have procedures regarding key IT security requirements necessary to protect the data accessed through the GSA Google and VDI accounts, including steps that GSA employees and GLS contractors should take when a contractor employee:

- Leaves a brokerage firm, including making the broker employee's security clearance inactive and removing access to G-REX, GSA Google, and VDI; and
- Moves to a different GLS brokerage firm.

The absence of clear procedures regarding the GLS contracts' IT security requirements limited GSA's assurance that government data was protected from theft, loss, or improper usage. Accordingly, GSA should evaluate other PBS contracts under which contractors are accessing government data using GSA Google and VDI accounts to ensure the appropriate guidance is in place.

Conclusion

We found that GSA did not appropriately administer the IT security requirements of the GLS contracts. GSA significantly changed the contractors' IT security obligations in the contract solicitation after contract award by providing GLS contractors with GSA Google and VDI accounts in lieu of requiring contractors' systems to meet federal IT security requirements. As a result, GSA made a cardinal change to the contracts and violated the Competition in Contracting Act and the FAR.

Further, GSA's actions limited its assurance that government data maintained on contractor systems was sufficiently protected. Until the contractors' transition to GSA Google and VDI was complete, GSA officials should have administered the terms and conditions of the original contract.

PBS issued the draft solicitation for the pending GLS Plus contract on December 19, 2018, and plans to issue the final solicitation in March 2020. To avoid a similar violation of federal competition requirements for this procurement of broker services, PBS should take steps to coordinate with GSA IT regarding the necessary IT requirements. PBS should also take steps to identify other contracts through which contractors access data through GSA Google and VDI accounts and ensure the proper terms, conditions, and guidance are in place to protect the government.

Recommendations

We recommend that the Commissioner, Public Buildings Service:

1. Coordinate with GSA IT to ensure that the IT requirements and solutions for the pending GLS Plus real estate broker solicitation accurately reflect the actual IT security requirements for contractor performance.
2. Identify other Public Buildings Service contracts through which contractors access government data through GSA Google or Virtual Desktop Interface accounts to ensure:
 - a. The contracts include terms and conditions necessary to protect the data; and
 - b. Guidance is in place defining roles and responsibilities governing compliance with applicable IT security requirements.

GSA Comments

In his response, the Commissioner of the Public Buildings Service agreed with our recommendations. The Commissioner's written comments are included in their entirety as **Appendix B**.

Audit Team

This audit was managed out of the Real Property and Finance Audit Office and conducted by the individuals listed below:

Marisa A. Roinestad	Associate Deputy Assistant Inspector General for Auditing
Timothy Keeler	Audit Manager
Arthur Edgar	Audit Manager
Gary Vincent	Auditor-In-Charge
John Foss	Management Analyst

Appendix A – Scope and Methodology

We reviewed the award and administration of the nine GLS contracts awarded September 30, 2015, from Solicitation Number GS-00-P-15-BQ-D-7002. Specifically, we reviewed the IT security requirements of the solicitation and contracts to determine whether GSA and the GLS contractors complied with those requirements.

To accomplish our objective, we:

- Interviewed management and contracting staff in PBS's Center for Broker Services who are responsible for the award and administration of the GLS contracts;
- Interviewed the GSA IT Information System Security Manager for the contracts;
- Reviewed the GLS contract files through the PBS eViewer system, to examine the acquisition plan, source selection plan, and contractor evaluations;
- Reviewed the GLS solicitation and amendments available on the Federal Business Opportunities website;
- Reviewed the cure notice issued to a GLS contractor and discussed the issue with the contracting officers;
- Reviewed GSA's assessments of contractor systems and letters issued to the GLS contractors authorizing the use of each system;
- Reviewed the 17 IT security deliverables provided by four contractors in Fiscal Year 2016 and Fiscal Year 2017 as required by Section H.3.4.4 of the GLS contracts; and
- Reviewed procedures to activate and de-activate GSA Google and VDI accounts and monitor user activity.

We conducted the audit between June 2017 and May 2018 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Internal Controls

Our assessment of internal controls was limited to those necessary to address the objective of the audit.


Appendix B – GSA Comments



Public Buildings Service

March 8, 2019

MEMORANDUM FOR MARISA A. ROINESTAD
ASSOCIATE DEPUTY ASSISTANT INSPECTOR
GENERAL FOR AUDITING
REAL PROPERTY AND FINANCE AUDIT OFFICE (JA-R)

FROM: DANIEL W. MATHEWS 
COMMISSIONER
PUBLIC BUILDINGS SERVICE (P)

Subject: Response to the Office of Inspector General (OIG) draft report,
*Audit of IT Security Requirements in GSA Leasing Support
Services Contracts – (A170092)*

This memorandum provides the Public Building Service's (PBS) response to the above audit report. PBS appreciates the opportunity to review and comment on this report.

OIG made the following recommendations:

- 1) Coordinate with GSA Office of Information Technology (IT) to ensure that the IT requirements and solutions for the pending Global Leasing Support (GLS) Plus real estate broker solicitation accurately reflect the actual IT security requirements for contractor performance.
- 2) Identify other contracts through which contractors access Government data through GSA Google or Virtual Desktop Interface (VDI) accounts to ensure:
 - a) the contracts include terms and conditions necessary to protect the data; and
 - b) guidance is in place defining roles and responsibilities governing compliance with applicable IT security requirements.

PBS concurs with the two recommendations. Regarding the second recommendation, PBS sought clarification from OIG concerning the scope of the contracts requiring review. Given the breadth of contracting performed by PBS and the GSA Office of IT, conforming to this recommendation has potentially significant resourcing implications. It was determined that contracts awarded and administered PBS-wide would be in scope for the purposes of the recommendation. Further, it was determined that GSA Office of IT and the PBS Office of Acquisition Management would develop a risk-based methodology for determining that PBS meets the intended outcome of the recommendation. This methodology will be addressed in the forthcoming Corrective Action Plan.

Should you have any questions, please contact Ken Schelbert, kenneth.schelbert@gsa.gov, 202-501-1109.

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

Appendix C – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

Commissioner (P)

Deputy Commissioner (P)

Chief of Staff (P)

Assistant Commissioner, Office of Leasing (PR)

Division Director, Lease Project Management and Tools Division, Office of Leasing (PRA)

Director, Center for Broker Services, Office of Leasing (PRAA)

Program Advisor, Office of Leasing (PRBA)

Associate CIO for Public Buildings Information Technology Services (IP)

Director of Financial Management (BG)

Chief Administrative Services Officer (H)

Audit Management Division (H1EB)

Assistant Inspector General for Auditing (JA)

Director, Audit Planning, Policy, and Operations Staff (JAO)