Audit Report

**REVIEW OF THE
IMPLEMENTATION OF GSA'S
IT INFRASTRUCTURE SUPPORT SERVICES
CONSOLIDATION INITIATIVE
REPORT NUMBER A070113/O/T/F09007**

June 18, 2009

Office of Inspector General
General Services Administration

Office of Audits

**REVIEW OF THE
IMPLEMENTATION OF GSA'S
IT INFRASTRUCTURE SUPPORT SERVICES
CONSOLIDATION INITIATIVE
REPORT NUMBER A070113/O/T/F09007**

June 18, 2009

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: June 18, 2009

Reply to   Gwendolyn A. McGowan
Attn of: Deputy Assistant Inspector General for Information Technology Audits
             (JA-T)

To: Casey Coleman
             Chief Information Officer (I)

Subject: Review of the Implementation of GSA's IT Infrastructure Support Services
             Consolidation Initiative
             Report Number A070113/O/T/F09007

This report presents a summary of the results of our audit of the General Services Administration's (GSA) Infrastructure Technology Global Operations (GITGO) consolidation initiative. The report highlights our audit findings and recommendations to the Agency's Office of the Chief Information Officer (OCIO) for improving the security, service, and cost validation of the consolidated infrastructure support services. With the GITGO initiative, the GSA OCIO is moving the Agency toward a standard, enterprise-wide resource management framework to establish and sustain effective and efficient information technology (IT) infrastructure support services. Accordingly, our review focused on risk areas where additional management attention may be needed to ensure that lessons learned with GITGO are adequately addressed to support GSA's information technology project management goals. We coordinated closely throughout the audit with program officials responsible for the GITGO implementation and carefully considered controls for managing security, service, and costs associated with the infrastructure support services. On March 30, 2009, we provided our preliminary findings and recommendations in a presentation to you and your staff. We have incorporated information that you provided and a copy of our updated briefing slides is contained in Appendix A. Due to the sensitive nature of the detailed findings in the appendix, we are restricting distribution of that information to your office.

Background

The GITGO performance-based task order was awarded to Catapult Technology, Ltd. on February 28, 2007 for the purpose of consolidating GSA's IT infrastructure support services. With GITGO, 40 existing contracts with approximately $59 million in annual infrastructure support costs were consolidated into a single contract valued at approximately $40 million annually. Program management, IT Service Desk/Help Desk, and local support services sub-tasks are firm fixed-priced, and client management services and network operations sub-tasks are labor-hour contract line items. The GITGO initiative is part of GSA's Exhibit 300 capital asset plan and business case for enterprise infrastructure. The Exhibit 300 is required to coordinate Office of Management and Budget's (OMB) collection of agency information to ensure the

business case for investments are made and tied to the Agency's mission statements, long-term goals and objectives, and annual performance plans. GSA's phased implementation of GITGO services started with the contract award 12-month base period and continues with four 12-month option periods to consolidate the IT infrastructure support services. Expected benefits from the GITGO initiative to consolidate GSA's internal contracts for desktop computing, networking, messaging and other services were: (1) combining 40 disparate contracts into one consolidated contract; (2) enhancing efficiency by aligning functions performed by multiple organizations and locations; (3) establishing consistent IT infrastructure levels of service throughout GSA; (4) establishing a consolidated help desk for all IT infrastructure issues; (5) improving management controls over funding for IT infrastructure, as funding will be consistently documented and analyzed; and (6) simplifying enterprise efforts such as implementing new software versions, responding to various security issues, and maintaining asset inventories.

Objective, Scope, and Methodology

Our audit objective was to assess whether risks with GSA's consolidation of IT support services have been adequately mitigated by determining if: (1) the GSA Infrastructure Technology Global Operations (GITGO) initiative for IT infrastructure support consolidation is generating expected cost savings and other benefits; (2) GSA's consolidated IT Service Desk is operating effectively, efficiently, and securely; and (3) GSA and the GITGO contractor are developing and implementing Information Technology Infrastructure Library (ITIL) processes to align IT support services to customer needs. If not, what changes are needed to ensure successful implementation of the GITGO initiative?

We gathered and analyzed information related to security, IT Service Desk operations, and infrastructure support services costs, which included the GITGO performance work statement (PWS), deployment of the ITIL framework, funding and justifications, strategic goals and objectives, standard operating procedures, performance measures, and service level agreements (SLA).

We met with GITGO officials and customers from the Federal Acquisition Service (FAS), Public Buildings Service, and Office of Governmentwide Policy. We also met with GITGO contractor personnel and FAS officials responsible for the Information Technology Infrastructure Line of Business. We visited the GITGO IT Service Desk in Chambersburg, PA for an overview of operations. For our IT security assessment, we relied on commercial tools and agreed-upon-procedures in place with the GSA Chief Information Officer (CIO) to evaluate operations at the Unicenter Service Desk in St. Louis, MO. In January 2009, we also reviewed a limited sample of service desk tickets that included active tickets, tickets referred by FAS personnel, and tickets associated with malicious code.

We considered applicable statutes, regulations, policies, operating procedures, and industry best practices regarding the development and implementation of the GITGO infrastructure consolidation such as: the PWS for the General Services Administration Office of the Chief Information Officer (OCIO) GSA Infrastructure Technology Global Operations, awarded February 2007, Task Identification Number A06S47T0040; GSA Information Technology (IT) Security Policy, CIO P 2100.1D, June 2007; National Institute of Standards and Technology

(NIST) Special Publication (SP) 800-61, Revision 1, Computer Security Incident Handling Guide, March 2008; GSA Information Technology (IT) Capital Planning and Investment Control, CIO 2135.2A, September 2006; GSA Information Technology (IT) Capital Planning and Investment Control, CIO 2135.2B, November 2008; GSA Information Technology (IT) Governance, CIO 2130.1, November 2008; Gartner Toolkit: IT Service Desks Must Understand the Importance of First Contact Resolution, June 2007; OMB M-05-23 – Improving Information Technology (IT) Project Planning and Execution, August 2005; OMB M-05-04 – Policies for Federal Agency Public Websites, December 2004; ITIL Service Support Version 2.6, 2000; ITIL Service Delivery Version 2.4, 2001; GSA IT Strategic Plan 2009 - 2011, August 2007; The Clinger Cohen Act of 1996; and OMB A-94 – Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs, October 1992.

This audit work began in February 2007 and was completed by February 2009. We conducted our audit work 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 objectives.

Results in Brief

The expected benefits for implementing GITGO include the establishment of consistent IT infrastructure levels of service throughout GSA, a consolidated service desk/helpdesk for all IT infrastructure issues, and improvement of management controls for funding IT infrastructure. Our review identified findings related to security, service, and cost validation risks that could hinder long-term success for GITGO if not adequately addressed. We have identified security controls that need to be strengthened in the areas of web application, database, and operating system platform security in response to results of technical scanning and other testing. Specifically, important risk management activities for the Unicenter Service Desk infrastructure, including certification and accreditation, the assignment of an Information System Security Officer (ISSO), and completion of an IT contingency plan should be prioritized. We also found that comprehensive procedures are not yet in place for service desk handling of security incidents, and audit trails for the remote support solution used by the IT Service Desk are not being analyzed for suspicious activity. An official GSA governance body should be utilized to review and approve changes to service level agreements as needed to monitor the performance of the infrastructure support processes. The IT Infrastructure Library (ITIL) is the selected IT service management framework for GITGO. However, a GITGO-specific ITIL plan, with milestones, is needed for guiding the development and implementation of ITIL disciplines for improving GSA's IT infrastructure services. Enhanced procedures are needed for the consolidated IT Service Desk to improve day-to-day operations. Since procedures were not adequate for verifying the pre-consolidation cost baseline information, the OCIO should improve the cost validation process to ensure the accuracy of future cost baselines for monitoring infrastructure support services. Taking steps to ensure improvements with GITGO at this time will assist GSA in progressing toward more standardized processes, reliable infrastructure support services, and efficiencies in GSA operations. To address the identified risk areas, we

have made specific recommendations for improving security, service, and cost validation for the GITGO initiative.

Summary of Audit Findings

Completion of Important Risk Management Activities Could Provide Assurance of Required Security Controls

Some technical control testing has been performed by system security officials at the Unicenter Service Desk (USD); however, the USD infrastructure[1] is operating without assurance of key risk management activities such as the completion of a certification and accreditation (C&A) of system security controls, the assignment of an Information System Security Officer, and the development of an IT contingency plan. Steps taken with GITGO to manage key C&A activities for the USD infrastructure have not been sufficient to manage specific risks. GSA's IT Security Policy establishes requirements for system authorization, system roles and responsibilities, and IT contingency planning. Without the completion of these key risk management activities, system security officials may not be able to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the USD infrastructure.

Vulnerabilities Identified Could Be Mitigated Through More Secure Configurations for Portions of the IT Service Desk Infrastructure

Our tests found specific instances of vulnerabilities that could be mitigated through more secure configurations for the USD infrastructure. GSA's IT Security Policy establishes detailed requirements for ensuring adequate protection of GSA IT resources. However, hardening practices for the IT Service Desk were not adequate to comprehensively address risks in web applications, databases, and operating systems. Additionally, key IT security requirements were not addressed in the performance measures included in the Performance Work Statement. These vulnerabilities could expose the USD infrastructure to undue risks affecting the confidentiality, integrity, or availability of the IT Service Desk. The details of these vulnerabilities are security sensitive and have been provided in Appendix A.

Additional Guidance Could Better Equip the IT Service Desk with IT Security Incident Handling Responsibilities

We identified weaknesses with security incident handling for the IT Service Desk in the areas of incident reporting and incident mitigation. These weaknesses had two contributing causes. First, comprehensive procedures are not yet in place to guide service desk handling of security incidents. Second, GITGO security officials determined that service desk personnel were not assigned significant security responsibilities and, therefore, were not required to complete role-based training provided under GSA's IT Security Program. While all service desk personnel must complete GSA's IT Security Awareness training to maintain their GSA email accounts, this basic training does not address all security incident handling responsibilities for service desk personnel. The GSA-CIO has issued a procedural guide that documents the required incident handling process for all users of GSA IT resources, including contractor personnel who have

---

[1] For the purpose of this report, the USD infrastructure refers to the servers and applications supporting the IT Service Desk in St. Louis, MO.

access to GSA resources, or otherwise provide services to GSA that handle or process GSA data. Without a comprehensive incident handling capability, GSA may not be able to effectively mitigate the exploited weaknesses. The details of these weaknesses are sensitive in nature and are included in Appendix A.

Monitoring Audit Trails for the Remote Access Solution Could Assist in Detecting and Deterring Potential Unauthorized Activity
Audit trails for the remote support solution used by the IT Service Desk personnel were not analyzed for suspicious activity. GSA's IT Security Policy states that audit records must be reviewed frequently for signs of unauthorized activity and other security events. This is an important security control since audit trails are used to deter and detect unauthorized access to computer systems and to help reveal potential misuse. However, system officials stated that they were uncertain regarding which activities should be analyzed in the available audit trails. By not analyzing audit trails, unauthorized activity or other potential security breaches may not be avoided or detected.

Senior Management Review and Approval Could Improve Service Level Agreements
Under GITGO, service level agreements (SLA) are used for incentivizing certain metrics, including the performance of the IT Service Desk. SLAs document the boundaries and service level goals of the agreed-upon services that will be provided to a specific customer, and sets forth specific penalties if the service provider fails to provide the agreed-upon services or to meet the agreed-upon goals. The SLAs for GITGO were revised to modify the definition of First Contact Resolution to count tickets that have been dispatched correctly as resolved. According to Gartner[2], First Contact Resolution is "the most fundamental of all metrics." While a GSA governance body had a charter to review SLAs, the revised SLAs were negotiated but not formally approved. Further, the Information Technology Infrastructure Library (ITIL) recommends the following for service level agreements: "Generally speaking, the more senior the signatories are within their respective organizations, the stronger the message of commitment." Without senior management approval, SLAs may not be incentivizing the most effective metrics for GITGO operations. Senior management, including stakeholders from GSA's Services, Staff Offices, and Regions may not be held accountable for the selection of metrics for IT service support needs under GITGO.

Establishment of Milestones and Implementation Plan Needed to Realize Benefits from Selected IT Service Management Processes
The GITGO Performance Work Statement (PWS) states that GSA will adopt the following ITIL processes at a minimum: (1) Problem Management, (2) Incident Management, (3) Change Management, (4) Release Management and (5) Configuration Management. We discussed these processes with the OCIO and documentation was provided on the status of ITIL for GITGO. However, this documentation does not include milestones to develop and guide the implementation of selected ITIL processes. Our analysis identified that the reason milestones have not yet been developed was that the PWS did not include milestones for oversight for the phased implementation of ITIL. New major IT projects in the Federal government are required to establish baselines with clear schedule and performance goals. Without a detailed

---

[2] *Gartner Toolkit: IT Service Desks Must Understand the Importance of First Contact Resolution*, June 2007.

implementation plan that considers such project management requirements, GSA may not be able to adequately address risks for GITGO ITIL implementation or meet important goals for standardized processes and reliable infrastructure, as outlined in the GSA IT Strategic Plan.

More Consistent Response to Tickets Could Be Achieved Through Standard Procedures to Guide the IT Service Desk Operations
Trouble tickets are used by IT organizations to track the detection, reporting, and resolution of problems reported by its customers. The GITGO IT Service Desk receives an average of 18,300 trouble tickets per month. We reviewed a sample of 75 tickets that included: 46 active tickets, 4 tickets referred by Federal Acquisition Service personnel, and 25 tickets associated with malicious code. Our analysis identified inconsistencies in IT Service Desk ticket handling, which may lead to inefficiencies. Specifically, service desk personnel did not consistently identify related tickets, set ticket categories, or classify tickets as an issue or change order. Further, we identified tickets that were not resolved in a timely manner. These inconsistencies were due to incorrect routing of tickets or procedures that were not comprehensive. A performance objective stated in the PWS for the IT Service Desk is to deploy a consolidated, enterprise help desk resulting in a reliable delivery of service. In addition, the PWS states that a goal for the GITGO initiative is to develop and deploy agency approved standard processes. Inconsistent handling of incidents by the IT Service Desk could lead to difficulty in analyzing the effectiveness of IT Service Desk operations and may impact ability of the IT Service Desk to consistently resolve trouble tickets in a timely manner.

Enhancing the Process for Verifying Cost Baselines Associated with Infrastructure Support Services Could Improve Management Planning Decisions
The GSA-CIO has consolidated forty contracts with annual infrastructure support costs of approximately $59 million into a single contract at approximately $40 million annually with GITGO. Agency officials did not verify the accuracy of the pre-consolidation cost baseline and did not conduct an independent validation for the baseline. This was due to OCIO procedures that were not adequate for verifying the pre-consolidation cost baseline information. New major IT projects in the Federal government are required to ensure that cost, schedule, and performance goals are independently validated for reasonableness. Reasonable baselines should be accurate, relevant, timely, and complete. Additionally, OMB Circular A-94 stipulates that analyses should be explicit about the underlying assumptions used to arrive at estimates of future benefits and costs. These analyses should include a statement of the assumptions, the rationale behind them, and a review of their strengths and weaknesses. Redundant services may be in place because all services under the pre-existing contracts were not verified for the pre-consolidation baseline. In addition, scope creep could occur if the baseline does not include all required infrastructure support services. We were unable to examine GITGO costs in detail from the capital asset plans and business cases submitted in 2007 and 2008 to OMB because IT infrastructure support costs from GITGO were not delineated from overall IT infrastructure costs. The OCIO stated that they have been tracking the costs for the GITGO initiative since its award. To improve the cost validation process, the OCIO should improve the process for verifying this cost information to better ensure the accuracy of future cost baselines necessary for monitoring infrastructure support services.

<u>Recommendations</u>

We recommend that the General Services Administration, Chief Information Officer (GSA-CIO) improve GSA Infrastructure Technology Global Operations (GITGO) security controls by:

1. Enhancing IT security management of key certification and accreditation activities for the Unicenter Service Desk (USD) infrastructure to include:
    a. Completing the required certification and accreditation.
    b. Assigning an Information System Security Officer (ISSO).
    c. Developing an IT contingency plan in accordance with the IT Security Policy.

2. Addressing the security vulnerabilities for the USD infrastructure to include:
    a. Mitigating the identified vulnerabilities.
    b. Enhancing hardening procedures for web applications, databases, and operating system platforms.
    c. Ensuring that IT security performance measures allow for adequate oversight of the IT Service Desk by incorporating key requirements into the contracting process.

3. Improving the handling of IT security incidents by the IT Service Desk to include:
    a. Establishing comprehensive procedures for handling IT security incidents, including procedures for reporting and mitigating IT security incidents.
    b. Ensuring that IT Service Desk personnel have training in their specific responsibilities for handling IT security incidents.

4. Analyzing remote support solution audit trails for unauthorized activity and other security events.

We recommend that the GSA-CIO improve GITGO service delivery and support by:

5. Ensuring that a governance body reviews and approves the Service Level Agreements.

6. Providing additional oversight for the adoption of the Information Technology Infrastructure Library (ITIL) to include developing milestones for the implementation of the selected ITIL processes.

7. Enhancing procedures for IT Service Desk incidents to ensure that they are consistently handled.

We recommend that the GSA-CIO improve infrastructure support services cost monitoring by:

8. Improving the cost validation process to verify project costs.

Management Comments

The GSA-CIO concurred with all audit findings and recommendations. A copy of the CIO's comments is provided in its entirety as Appendix B.

Internal Controls

The objective of this review was to assess whether risks with GSA's consolidation of IT support services have been adequately mitigated by determining if: (1) the GSA Infrastructure Technology Global Operations (GITGO) initiative for IT infrastructure support consolidation is generating expected cost savings and other benefits; (2) GSA's consolidated IT Service Desk is operating effectively, efficiently, and securely; and (3) GSA and the GITGO contractor are developing and implementing Information Technology Infrastructure Library (ITIL) processes to align IT support services to customer needs. If not, what changes are needed to ensure successful implementation of the GITGO initiative? This report states the need to strengthen specific controls for GITGO security, services and cost validation to improve operations and customer satisfaction. This review did not address all of the expected benefits of the GITGO initiative.

I wish to express my appreciation to you and your staff for your cooperation during the audit. If you have any questions, please contact me or Gwen McGowan, Deputy Assistant Inspector General for Information Technology Audits, on 703-308-1223.
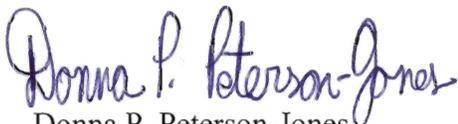
Donna P. Peterson-Jones
Audit Manager, Information Technology Audit Office (JA-T)

**REVIEW OF THE
IMPLEMENTATION OF GSA'S
IT INFRASTRUCTURE SUPPORT SERVICES
CONSOLIDATION INITIATIVE
REPORT NUMBER A070113/O/T/F09007**

APPENDIX A – BRIEFING SLIDES TO THE OCIO

Due to the sensitive nature of the detailed security information contained in this appendix, only reports provided to the Chief Information Officer (CIO) and appropriate officials of the Office of the Chief Information Officer contain a copy of the briefing slides used to present detailed information to the CIO on March 30, 2009. Requests for copies of these slides should be referred to Gwendolyn McGowan, Deputy Assistant Inspector General for Information Technology Audits, or Donna Peterson-Jones, Audit Manager, on 703-308-1223.

**REVIEW OF THE
IMPLEMENTATION OF GSA'S
IT INFRASTRUCTURE SUPPORT SERVICES
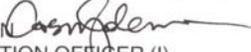CONSOLIDATION INITIATIVE
REPORT NUMBER A070113/O/T/F09007**

APPENDIX B – GSA CIO'S RESPONSE TO THE DRAFT REPORT

GSA

GSA Office of the Chief Information Officer

June 4, 2009

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

FROM: CASEY COLEMAN
                    CHIEF INFORMATION OFFICER (I)

SUBJECT: Draft Report: Review of the Implementation of GSA's IT
                    Infrastructure Support Services Consolidation Initiative
                    Report Number A070113/O/T

This is in response to the IG draft audit on the Review of the Implementation of
GSA's IT Infrastructure Support Services Consolidation Initiative Report Number
A070113/O/T.

My staff has reviewed the draft audit report and we concur with your audit
findings and recommendations.

If you or your staff has any questions or require additional information, please
contact Mike Seckar, on 202-208-5054.

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

REVIEW OF THE
IMPLEMENTATION OF GSA'S
IT INFRASTRUCTURE SUPPORT SERVICES
CONSOLIDATION INITIATIVE
REPORT NUMBER A070113/O/T/F09007

APPENDIX C – REPORT DISTRIBUTION

With Appendix A	Electronic Copies
Office of the Chief Information Officer (I)	3
Office of Enterprise Infrastructure (IO)	2

Without Appendix A	
Assistant Inspector General for Auditing (JA)	1
Director, Audit Operations (JAO)	1
Assistant Inspector General for Investigations (JI)	1
Internal Control and Audit Division (BEI)	1
Administration and Data Systems Staff (JAS)	1
Regional Inspector General for Auditing, National Capital Region (JA-W)	1