

AUDIT REPORT

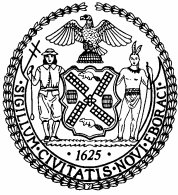


CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
BUREAU OF FINANCIAL AUDIT
WILLIAM C. THOMPSON, JR., COMPTROLLER

Audit Report on the Development and Implementation of the Capital Asset Management System By the Department of Citywide Administrative Services

7A06-112

June 29, 2007



THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, N.Y. 10007-2341

WILLIAM C. THOMPSON, JR.
COMPTROLLER

To the Citizens of the City of New York

Ladies and Gentlemen:

In accordance with the responsibilities of the Comptroller contained in Chapter 5, §93, of the New York City Charter, my office has audited the development and implementation of the Capital Asset Management System (CAMS) by the Department of Citywide Administrative Services.

CAMS is a Web-based capital planning and management software system. It contains detailed and comprehensive facility and infrastructure data for the 53 public buildings under the custodianship of the Department of Citywide Administrative Services. We audit systems and technological resources of City agencies such as this to ensure that they are cost-effective, efficient, secure, and operate in the best interest of the public.

The results of our audit, which are presented in this report, have been discussed with officials of the Department of Citywide Administrative Services, and their comments have been considered in preparing this report. Their complete written responses are attached to this report.

I trust that this report contains information that is of interest to you. If you have any questions concerning this report, please e-mail my audit bureau at audit@Comptroller.nyc.gov or telephone my office at 212-669-3747.

Very truly yours,

A handwritten signature in cursive script that reads "William C. Thompson, Jr.".

William C. Thompson, Jr.

WCT/fh

Report: 7A06-112
Filed: June 29, 2007

Table of Contents

AUDIT REPORT IN BRIEF	1
INTRODUCTION	3
Background	3
Objectives	4
Scope and Methodology	4
Scope Limitation	5
Discussion of Audit Results	6
FINDINGS AND RECOMMENDATIONS	7
VFA's Management of CAMS Has Not Been Monitored or Reviewed by DCAS	7
Disaster-Recovery Information Is Not Comprehensive	8
Risk Assessments of System Security Have Not Been Performed	11
Review of Access Privileges Not Performed	13
APPENDIX The 53 Buildings Maintained by DCAS and Documented as Being Part of the CAMS Database	
ADDENDUM Department of Citywide Administrative Services Response	

*The City of New York
Office of the Comptroller
Bureau of Financial Audit
IT Audit Division*

**Audit Report on the
Development and Implementation of the
Capital Asset Management System by the
Department of Citywide Administrative Services**

7A06-112

AUDIT REPORT IN BRIEF

This audit examined the development and implementation of the Capital Asset Management System by the Department of Citywide Administrative Services (DCAS). DCAS is responsible for ensuring that City agencies have the critical resources and support needed to provide the best possible services to the public. DCAS supports City agencies' needs in recruiting, hiring, and training employees; provides overall facilities management, including security, maintenance, and construction services for 53 public buildings; purchases, sells, and leases non-residential real property; and purchases, inspects, and distributes supplies and equipment.

On September 1, 2003,¹ DCAS contracted with Aramark Facility Services, Inc., (Aramark) to provide a Web-based capital planning and management software system known as the Capital Asset Management System (CAMS). DCAS procured CAMS through a New York State Office of General Services, Building Commissioning and Asset Management Services contract. As part of the contract, DCAS agreed that Aramark could use Vanderweil Facility Advisors, Inc., (VFA) as its subcontractor. VFA was to provide a detailed and comprehensive facility and infrastructure condition assessment of the 53 public buildings that were under the custodianship of DCAS. CAMS is currently installed and maintained by VFA at the AT&T Internet Data Center in Boston, Massachusetts. DCAS has not formally accepted the system as being completed because the data that was collected by VFA for each building is currently under review by the Division of Facilities Management and Construction.

Audit Findings and Conclusions

We could not conclude that CAMS as a finished product meets the overall goals as stated in the system justification, nor can we determine whether it meets the initial business and system

¹ Dated October 8, 2003

requirements as specified by DCAS. However, the system is operational. In addition, DCAS has not formally accepted the system as being completed, asserting that the system would be accepted once information in the database is fully reviewed. Further, as DCAS did not provide supporting documentation, we could not substantiate the accuracy of the CAMS data, thus leaving unanswered the potential exposure of DCAS to inaccurate information.

VFA currently operates CAMS at the AT&T Internet Data Center in Boston, Massachusetts; however, VFA's disaster-recovery plan is not specific, and documentation of a comprehensive test for disaster recovery was not provided. Moreover, security assessments have not been performed. Also, DCAS representatives did not review the access privileges of individuals employed by VFA who had access to CAMS. Nor did DCAS review VFA operational procedures and controls to ensure they were in accord with acceptable City standards.

Finally, VFA followed a formal methodology when it installed CAMS; CAMS allows for future enhancements and periodic upgrades; and DCAS generally complied with the applicable City Charter provisions and PPB rules when procuring the system.

Audit Recommendations

To address these issues, we recommend that DCAS:

- Immediately perform an on-site review of VFA operation to ensure that VFA's policies and procedures comply with DOI Directives.
- Request from VFA the primary elements of the disaster-recovery plan for the CAMS system; and
- Ensure that the disaster-recovery plan is tested in accordance with DOI Directives.
- Perform an initial security-risk assessment of CAMS and then each year thereafter or when a major change to the system application is implemented;
- Ensure adherence to applicable directives and standards identified during the security-risk assessment process; and
- Perform a security-risk assessment of the alternate hosting site, if one is under consideration.
- Create a formal procedure for DCAS and VFA for the periodic review of user privileges to ensure their appropriateness and make corrections as needed.

INTRODUCTION

Background

The Department of Citywide Administrative Services (DCAS) is responsible for ensuring that City agencies have the critical resources and support needed to provide the best possible services to the public. DCAS supports City agencies' needs in recruiting, hiring, and training employees; provides overall facilities management, including security, maintenance, and construction services for 53 public buildings; purchases, sells, and leases non-residential real property; and purchases, inspects, and distributes supplies and equipment.

On October 4, 2002, DCAS issued a Project Definition² for a capital-asset management system to provide "a centralized database of the agency's capital assets, sophisticated analysis and reporting functions," and to serve as a comprehensive budgeting tool. The goals of the project are to:

- "Provide a complete assessment of DCAS' buildings' infrastructure.
- "Establish a defensible lifecycle for DCAS buildings and components.
- "Integrate building information with a system to support management decisions.
- "Produce a multi-year capital budget that accurately reflects DCAS infrastructure needs."

On September 1, 2003, DCAS contracted with Aramark Facility Services, Inc., (Aramark) to provide a Web-based capital planning and management software system known as the Capital Asset Management System (CAMS). CAMS is an off-the-shelf product that has been in use in the business world for more than seven years. As part of the contract, DCAS agreed that Aramark could use Vanderweil Facility Advisors, Inc., (VFA) as its subcontractor. VFA was responsible for installing, and maintaining CAMS in accordance with the contract. Specifically, VFA was to provide a detailed and comprehensive facility and infrastructure condition assessment of the 53 public buildings that were under the custodianship of DCAS, resulting in a Web-based database comprising all data collected during this assessment, and a fully operational capital planning and management software system. CAMS is Web-based, and it is currently installed and maintained by VFA at the AT&T Internet Data Center in Boston, Massachusetts. DCAS personnel can access and update information on CAMS only through the CAMS Internet Web site.

DCAS procured CAMS through a New York State Office of General Services, Building Commissioning and Asset Management Services contract, a procedure that is in accordance with City Procurement Policy Board (PPB) rules. The terms of the contract stated a total cost of \$3 million. Through August 2006, the end of this audit's scope period, DCAS spent \$1,677,506.43. However, DCAS has not formally accepted the system as being completed because the data that was collected by VFA for each building is currently under review by the Division of Facilities Management and Construction.

² A Project Definition provides historical information, available industry research, initial scope, a rough schedule, and implementation plans for the proposed project. It also outlines business objectives of the project.

Objectives

The objectives of the audit were to determine whether CAMS:

- As a finished product, meets overall goals as stated in the system justification;
- Meets DCAS initial business and system requirements;
- Design allows for enhancements and upgrades;
- Was developed using a formal system development methodology;
- Functions reliably, and information recorded in the database is accurate and is secure from unauthorized access;
- Was procured in accordance with City Charter provisions and PPB rules; and
- Has a disaster-recovery plan, and whether this plan has been incorporated into the overall disaster-recovery plans of DCAS.

Scope and Methodology

Our fieldwork was conducted between March 2006 and August 2006. To achieve our audit objectives, we interviewed DCAS and VFA officials and:

- Reviewed specification documents, contracts, and other system-related documentation;
- Conducted a system walk-through on August 9, 2006, to review how CAMS functions;
- Requested the assessment source documents and all recent changes to initial data entered in CAMS from which to select a random sample of 10 of the 53 public buildings maintained by DCAS and documented as being part of the CAMS database; and used the sample to test the accuracy of the data stored in CAMS;
- Logged on to the CAMS Web site to test system-access security;
- Reviewed DCAS and VFA CAMS user-access lists to assess whether access privileges were appropriate;
- Prepared and requested answers to a series of inquiries and questions to DCAS representatives the purpose being to clarify and explain various elements of the development.

- Prepared and requested answer to a series of inquiries and questions to VFA representatives in Boston the purpose being to clarify and explain various elements of the development.
- Tested compliance with all applicable City Charter provisions and PPB criteria, including provisions for using state contracts; and
- Reviewed VFA disaster-recovery and contingency-planning procedures.

As criteria, we used the Department of Investigation (DOI) Citywide Information Security Architecture Formulation and Enforcement (CISAFE) *Information Security Directive*, the National Institute of Standards and Technology (NIST) Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, and all relevant sections of the City Charter provisions and PPB rules. Since the City has no stated formal system-development methodology, as criteria we used NIST Special Publication 500-223, *A Framework for the Development and Assurance of High Integrity Software* and the New York City Comptroller’s Internal Control and Accountability Directive #18, “Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems,” to ascertain whether DCAS followed a formal methodology.

Scope Limitation

DCAS officials did not provide us with the supporting documentation needed to test the accuracy of the data in CAMS, asserting that the system would be accepted once information in the database is fully reviewed. Consequently, we could not test whether the data entered into CAMS is accurate. Therefore, we were unable to conclude whether CAMS as a finished product, meets the overall goals as stated in the system justification. In this regard, we were also unable to determine whether CAMS meets the initial business and system requirements as specified by DCAS. We intended to test data accuracy by verifying the accuracy of the data that should have been in CAMS for 10 buildings that we randomly selected. We requested the assessment source documents and all recent changes to that initial data for our sample of 10 buildings. To ensure that the data was appropriately approved by DCAS officials, we requested evidence of formal approval of the assessment data by DCAS architectural and engineering specialists. We did not receive the supporting documentation requested.

DCAS Response: “We believe . . . in the ‘Scope Limitation’ discussion, the Report states that ‘DCAS officials did not provide us with the supporting documentation needed to test the accuracy of the data in CAMS . . .’ The Auditors had requested the raw data collected by the consultant personnel during their walk-through of the buildings. This statement gives the impression that we did not cooperate in this manner, which is not accurate. We did not provide this data because we do not have it.

“Prior to issuing individual building reports for DCAS review and comment, the consultant, VFA, subjected the information to a quality review process. This process included validating costs by comparing them against the costs for other, similar buildings. In addition, multiple teams were used to cross-check the work of the people who visited

the property. Therefore, the review of the raw data, a condition prior to the consultant's quality review, will not provide any valid indication of the accuracy of the data in CAMS. It is only the subsequent review of these judgments by other qualified personnel, as we are currently performing, that will ultimately address that issue."

Auditor Comment: DCAS officials concur that they did not provide us with the requested source documentation that would have permitted us to determine whether the information in CAMS was accurately and properly entered. Accordingly, the lack of source documentation for examination precluded our fulfilling our audit objectives and assessing the accuracy of the system's data. DCAS's contention that it did not have the data is misleading, given that the CAMS system is already being used by agency personnel. Although the DCAS consultant may be conducting a "quality review" of this data, it is difficult to comprehend that DCAS would not maintain documentation of information that has been entered in CAMS, a system that has not yet been accepted as complete and is still considered a work in progress. Further, in its response, DCAS acknowledges that this data was in fact furnished to DCAS architectural and engineering personnel for the final review. Therefore, the data that DCAS states it does not have was given to DCAS personnel but was not made available to us to examine and test to complete our review.

This audit was conducted in accordance with generally accepted government auditing standards (GAGAS) and included tests of the records and other auditing procedures considered necessary. This audit was performed in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, §93, of the New York City Charter.

Discussion of Audit Results

The matters covered in this report were discussed with DCAS officials during and at the conclusion of this audit. A preliminary draft report was sent to DCAS officials and discussed at an exit conference held on March 2, 2007. On March 14, 2007, we submitted a draft report to DCAS officials with a request for comments. We received a written response from DCAS officials on April 4, 2007.

In their response, DCAS officials disagreed with a number of the audit's findings and conclusions. DCAS believes that there are misinterpretations and disagreements between the auditors and the agency about the CAMS project. Specifically, DCAS contends that the audit "handles" CAMS as if it were an information technology project, whereas DCAS characterizes it as an engineering project. Nevertheless, our audit examination was intended to determine whether the project: was monitored to ensure its timely completion; was properly controlled to ensure that information was accurately stored; and contained information that was adequately protected. Thus, our review indicated that DCAS did not fulfill these project-management objectives, regardless of the project's characterization as an information technology project or an engineering one.

The details of the DCAS comments and our responses to them are incorporated in the related section of the report. The full text of the DCAS comments is included as an addendum to this report.

FINDINGS AND RECOMMENDATIONS

We could not conclude that CAMS as a finished product meets the overall goals as stated in the system justification, nor can we determine whether it meets the initial business and system requirements as specified by DCAS. However, the system is operational. In addition, DCAS has not formally accepted the system as being completed, asserting that the system would be accepted once information in the database is fully reviewed. Further, as DCAS did not provide supporting documentation, we could not substantiate the accuracy of the CAMS data, thus leaving unanswered the potential exposure of DCAS to inaccurate information.

VFA currently operates CAMS at the AT&T Internet Data Center in Boston, Massachusetts; however, VFA's disaster-recovery plan is not specific, and documentation of a comprehensive test for disaster recovery was not provided. Moreover, security assessments have not been performed. Also, DCAS representatives did not review the access privileges of individuals employed by VFA who had access to CAMS. Nor did DCAS review VFA operational procedures and controls to ensure they were in accord with acceptable City standards.

Finally, VFA followed a formal methodology when it installed CAMS; CAMS allows for future enhancements and periodic upgrades; and DCAS generally complied with the applicable City Charter provisions and PPB rules when procuring the system.

VFA's Management of CAMS Has Not Been Monitored or Reviewed by DCAS

As stated previously, CAMS is Web-based; it is currently installed and maintained by VFA at the AT&T Internet Data Center in Boston, Massachusetts. DCAS personnel can access and update information on CAMS only through the CAMS Internet Web site. In that regard, DCAS has relinquished control over the development and maintenance of the system to VFA. While this relationship between DCAS and VFA allows DCAS personnel some efficiency, which saves time, DCAS has not reviewed the work provided by VFA.

In fact, scheduled periodic meetings between DCAS and VFA personnel have not taken place since 2004. The lack of consistent monitoring of the vendor leads us to question whether DCAS can be assured that VFA's operation has adequate internal controls. These internal controls should include, but are not limited to, controls over application programs and operating-system maintenance; access to data files and program libraries; standardized procedures in computer operations and ensuring that those procedures are actually followed; and application controls.

DOI Directive 5.1, §3.3, states, "Where administrative responsibility for network resources is outsourced to vendors, the City agency must retain the responsibility for reviewing network and vendor performance. Network administrators must meet periodically with vendors and review vendor-provided reports and logs."

DCAS Response: “We are troubled by the statement in the Report that ‘scheduled periodic meetings between DCAS and VFA have not taken place since 2004,’ as we believe that the reader is left with the impression that the project has been languishing. As a point of clarification, we believe that such regular face-to face meetings, which were appropriate when consultant personnel were already in New York performing surveys of the buildings, are far less efficient and desirable when the consultant personnel are not otherwise scheduled to be in New York City. Rather, we determined that beyond the initial project phase, incurring additional travel and lodging costs to hold face-to-face meetings was generally unnecessary and fiscally irresponsible. Therefore, taking advantage of modern technology, we have increasingly handled most of our meetings via telephone, email, and teleconferences, supplemented by face-to-face meetings whenever they are prudent. A cursory examination of our records indicates that additional face-to-face meetings took place on the following dates: 9/29/2005, 10/18/2005, 12/12/2005, 11/21/2005, and 8/09/2006. Teleconferences were held on: 12/14/2005, 7/06/2006, 11/20/2006 and 01/29/2007. These meetings are in addition to numerous communications between the Project Manager and the consultant by telephone and email.”

Auditor Comment: As stated previously, our audit found that DCAS failed to consistently monitor its project vendor VFA to ensure the adequacy of the vendor’s internal controls. While DCAS responded that it held various meetings and teleconferences with VFA, we did not find any documentation to substantiate the dates of these meetings or that the purported meetings dealt with any aspects of monitoring per se. In fact, DCAS officials informed us during the course of our audit that they did not monitor or receive periodic reviews and updates from VFA. Moreover, in response to our August 4, 2006 request for documentation, VFA stated that it did not routinely meet with DCAS, and that meetings would not occur until the development of a final implementation plan. Finally, there was no documentation to indicate that DCAS had examined VFA operations in Boston.

Recommendation

DCAS should:

1. Immediately perform an on-site review of VFA operation to ensure that VFA’s policies and procedures comply with DOI Directives.

DCAS Response: See response to Recommendations 2 and 3.

Disaster-Recovery Information Is Not Comprehensive

Although VFA stated that CAMS is included in its disaster-recovery plan, we found that the disaster-recovery information was not comprehensive. The plan information that was provided by VFA did not include the primary elements of a recovery in accordance with DOI

Directive 2.13, §2.2, which states, “The primary elements of a recovery plan include but are not limited to . . .

- “The steps the City agency will take to determine whether an event is sufficiently “serious to implement the plan.
- “A prearranged agreement describing the conditions under which a disaster is to be declared.
- “The names, telephone numbers, and specific responsibilities of each individual involved in a disaster situation.
- “Specific business and disaster recovery procedures. . . .
- “The order of priority in which information systems must be reinstated.
- “Equipment and software supply agreements.
- “Recovery-assistance consultants.
- “Hot site, cold site, service bureau, or reciprocal arrangements.
- “Periodic testing of the BCP” (Business Continuity Plan).”

Also, VFA stated that no annual comprehensive test of the disaster-recovery plan was performed, and it has not included its plan in the DCAS BCP. An untested and undocumented recovery plan increases the risks of failures to process and access records should a disaster occur. DOI Directive 2.13, §2.6, states, “If a City agency receives services from a data center it does not own or operate, the City agency must insist that the service bureau has adequate business continuity planning. Furthermore, the agency must ensure that the service bureau’s plan is tested annually and must incorporate it into the City agency’s own BCP.”

DCAS Response: “3. The requirements of the data in a computer system determine the appropriate level of security for that application. [Emphasis in original.] The important concept is that information security is not a ‘one size fits all’ proposition. There are some computer systems that, due to the very sensitive nature of the data that they contain, or the extremely critical nature of the system itself, will require extraordinary measures to protect that data. Conversely, there are less sensitive systems containing less sensitive information that will merit a diminished level of expense or effort to secure their information. The instant system falls within the latter category.

“During the course of the Audit, we informed the auditors that we had carefully evaluated the CAMS information and had judged it to be neither sensitive, nor critical, as defined by City Comptroller Directive #18. Consistent with our evaluation of this data, we took appropriate security steps, as well as steps to ensure that the data would not be lost and could be recovered if corrupted or otherwise unavailable. This precaution entails both keeping a hard copy and electronic copies of the data on-site, in addition to the copy maintained by VFA at the ATT datacenter in Boston. Furthermore, the DCAS electronic copies of the data will also be stored on a DCAS server, which is backed-up to the DoITT [Department of Information Technology and Telecommunications] datacenter, and covered under both our disaster plans. This would provide a data library that would be comprised of at least five (5) distinct copies of the data, each covering multiple time periods allowing for restoration of the data to a prior period if necessary. Therefore, even

if this vendor were to fail or if its disaster plan would prove to be inadequate, we are assured that the data will be available for our use.

“Contrary to our view that we need to provide appropriate security measures at the best cost, the Report suggests that we should seek out the best level of security available for this system, and ‘choose the vendor that will ensure optimal conditions with which to operate the system.’ This is apparently to be done without consideration of cost or necessity. It is our opinion that before we spend an excessive amount of time or inordinate amount of taxpayer money to bring CAMS into line with a more stringent security environment, it would be necessary to articulate the need so as to justify the additional benefits being purchased. We believe the level of security established is appropriate, justifiable, and cost-effective.”

Auditor Comment: DCAS’s response is misleading. The audit finding pertains to DCAS’s compliance with DOI’s Directive 2.13, §2.2 — not with the price, sensitivity, or nature of the system data. Accordingly, DCAS must ensure that the disaster-recovery plan is comprehensive, contains all required elements, and uses the resources needed for ensure adequate security.

Recommendations

DCAS should:

2. Request from VFA the primary elements of the disaster-recovery plan for the CAMS system; and
3. Ensure that the disaster-recovery plan is tested in accordance with DOI Directives.

DCAS Response: “Responses 1–3: We believe that we have addressed these issues through the use of internal controls. Specifically, we will require VFA to provide us with a back-up of our data at regular intervals, following our major updates to this data. The backup will be stored on site at DCAS, and will be archived on our in-house server, which is, in turn, backed up to DoITT on a daily basis, and covered under their disaster plan. This procedure will provide us with copies of the data on the live VFA system at the ATT datacenter in Boston, at the VFA back-up site in Boston, and also a library of warehoused copies at DCAS and at DoITT, in addition to the hard copy data that we also have in-house.

“In addition, the data will be formed into discrete capital projects and entered into the FMS Four and Ten- Year Capital Plans. FMS is housed at the FISA datacenter.

“Therefore even if this data were to become corrupt due to VFA weaknesses, or if a disaster were to strike their datacenter, or if their disaster plan was found to be inadequate, we can be confident that we will not lose our data.

“We will, however, follow up with the consultant regarding the testing of its disaster plan.”

Auditor Comment: As stated previously, DCAS personnel have never performed an on-site review of VFA’s operation. The DCAS response consistently remains mute on that point. Further, in its response to our June 8, 2006 questionnaire, DCAS specifically indicates that VFA does not provide DCAS management with security reports, operational reports, and statistical reports regarding the day-to-day operations of CAMS. Therefore, DCAS cannot substantiate its assertion that their internal controls can address all the control issues of an off-site operation.

Also, DCAS is cognizant that there has been: (1) no on-site review of the VFA facility to ensure adequate controls are in place; (2) no comprehensive test of the CAMS disaster-recovery plan; (3) no security reports, operational reports, and statistical reports regarding the day-to-day operations of CAMS provided to DCAS; (4) no Risk Assessment that has been completed; (5) no final approval as to the accuracy of the data; and (6) no final acceptance of the project. Therefore, there is no independent information on the CAMS environment. In that regard, we question how DCAS can be confident that it can make any informed statements about the system’s electronic or hard-copy data.

Risk Assessments of System Security Have Not Been Performed

A security risk assessment has not been performed on CAMS. DCAS officials asserted that since CAMS is being hosted at a data center of a private entity outside New York City, the system would fall under the security plans of the host center. However, DCAS officials could not demonstrate that the City security requirements were being met by VFA at the AT&T Internet Data Center in Boston. Consequently, should the security at the host center be inadequate, these sites (specifically, the specifications for these building)³ are at risk of access by unauthorized individuals.

DOI Directive 2.1, §1, states, “Information Security Risk Assessments, information classifications, and the ensuing compliance reviews are processes recommended to the City agencies, in order to mitigate risks related to monetary loss, productivity loss, and loss of public confidence (embarrassment).”

According to DOI Directive 2.1, §3, “full Information Security Risk Assessment constitutes a completion of the eight steps . . . :

1. “Step One: Risk Assessment Data Sheet
2. “Step Two: Personnel
3. “Step Three: Facilities and Equipment
4. “Step Four: Communications
5. “Step Five: Applications
6. “Step Six: Environmental Software and Operating Systems

³ See Appendix for list of buildings managed by DCAS.

7. “Step Seven: Compilation of Risks on the Risk Assessment Matrix
8. “Step Eight: Assignment of Composite Risk Levels”

Only after a security-risk assessment is performed on CAMS can DCAS determine which security requirements apply to CAMS. DOI Directive 2.1, §1, states, “When the Information Security Risk Assessment process has been completed for an application, system, or business process, an Information Security Directives and Standards compliance review is undertaken. The compliance review is performed to judge adherence to the identified Directives and Standards.”

Only after an initial security-risk assessment is conducted and security requirements are properly defined and implemented can DCAS then ensure that an adequate security-risk assessment is performed on CAMS and that it is performed on an annual basis or when a major change to the system application is implemented. In this regard, DOI Directive 2.1, §2.2.2, states, “The Information Security Risk Assessments must be performed on a yearly basis or whenever a change occurs in the way information is input, processed, or output by an application, system, or business process. After performing the initial Information Security Risk Assessment, subsequent assessments usually require substantially less time and fewer resources to complete.”

Finally, although the contract ended on August 31, 2006, DCAS has not accepted the CAMS project. A DCAS memorandum, dated July 13, 2006, indicates, “This system will be accepted as complete by DCAS when upon completion of the review of the information contained in the database and upon resolution [of] the recent software difficulties.”⁴ Once the project is completed and accepted, DCAS has to decide whether to maintain the system with VFA or with another vendor at an alternate hosting site. Currently, VFA is providing hosting services for all data associated with this project. If DCAS is considering another vendor to host CAMS, DCAS needs to perform a security-risk assessment of the vendor’s data center site. By performing a security assessment on the alternate site, DCAS can compare and address the security concerns at each site and choose the vendor that will ensure optimal conditions with which to operate the system.

DCAS Response: “The Audit concludes that ‘[a] Security Risk Assessment has not been performed on CAMS.’ In fact, we have prepared a Risk Assessment document that is currently under discussion with the City’s Chief Information Security Officer (CISO) at the DoITT. That Office has advised us that our approach concerning CAMS security is not unreasonable. Once again, the fact that we are in the process of engaging in proper actions to finalize an ongoing project is not a deficiency.”

Auditor Comment: In response to our August 4, 2006 questionnaire, DCAS indicated that VFA did not perform a comprehensive test of their disaster-recovery plan. In addition, at the time of their response to this audit, DCAS has not completed the Risk

⁴ According to the DCAS memorandum, resolution of these system operations problems were addressed as follows: “VFA arranged for a visit by their IT staff to diagnose the problem. That visit occurred June 9th [2006]. Since that time, VFA has made some alternate arrangements to provide better operability, but is still working on the SSL [Secure Sockets Layer] latency problem.”

Assessment document on CAMS with DoITT. Also, DCAS has announced in its response that it has prepared a Risk Assessment document that is **currently** under discussion with the City's Chief Information Security Officer (CISO) at the DoITT. It should be noted that the Risk Assessment was started as a result of inquiries we made during the course of this audit. Therefore, based on these facts, we conclude that DCAS's belief that the CAMS security environment is "appropriate, justifiable, and cost-effective" is premature, and suggest that DCAS ensure that adequate security requirements apply to CAMS.

Recommendations

DCAS should:

4. Perform an initial security-risk assessment of CAMS and then each year thereafter or when a major change to the system application is implemented;
5. Ensure adherence to applicable directives and standards identified during the security-risk assessment process; and
6. Perform a security-risk assessment of the alternate hosting site, if one is under consideration.

DCAS Response: "Responses 4–6: We have prepared a Risk Assessment document that is currently under discussion with the City's Chief Information Security Officer (CISO) at DoITT. We expect to finalize this shortly. If we did not host this application with VFA, the alternative would be to explore hosting at the DoITT datacenter. Since the DoITT operation is under the direction of the City's CISO, we would not perform a security Risk Assessment.

"The current expectation is that we will continue the current hosting arrangement with VFA. However, we will continue to explore the security arrangements with the CISO at DoITT as well as DoITT's capability for hosting this application. Once complete we will revisit this analysis annually and update it if necessary."

Review of Access Privileges Not Performed

On August 30, 2006, we asked VFA to justify approvals for the list of 29 employees with full access to CAMS. In its response to this request, VFA removed access for 14 employees who previously had full access to the information on CAMS. VFA indicated that a "Full Access" user can view and edit the user list and user-access privileges. All 14 VFA employees had been involved in either the assessment or the training process during the system's development.

DCAS relies on VFA to have installed adequate internal controls and to monitor the user profiles of employees who have access to CAMS. In that regard, DCAS must perform a formal review to determine whether DCAS and VFA employees have the appropriate user profiles and

system-access required to complete the designated tasks for their job functions. Without such a formal review by DCAS system management of user profiles and system access, there is no assurance that VFA is maintaining systems security at an optimal level. The NIST *Generally Accepted Principles and Practices for Securing Information Technology Systems*, §3.5.2, states, “Organizations should ensure effective administration of users’ computer access to maintain system security, including user account management, auditing and the timely modification or removal of access.”

Recommendation

DCAS should:

7. Create a formal procedure for DCAS and VFA for the periodic review of user privileges to ensure their appropriateness and make corrections as needed.

DCAS Response: “We will regularly review all user privileges and make changes as necessary.”

Appendix

The 53 Buildings Maintained by DCAS and Documented as
Being Part of the CAMS Database

Buildings	Locations	Boroughs
Bronx Family/Criminal Court	215 E. 161st Street	Bronx
Bronx Supreme Court	851 Grand Concourse	Bronx
Bergen Building	1918-1932 Arthur Avenue	Bronx
Bronx Housing Court	1118 Grand Concourse	Bronx
Bronx Neighborhood Government Building	4101 White Plains Road	Bronx
Brooklyn Borough Hall	209 Joralemon Street	Brooklyn
Brooklyn Municipal Building	210 Joralemon Street	Brooklyn
Office of Transportation	Navy Yard	Brooklyn
OEM Command Center	11 Water Street	Brooklyn
345 Adams Street	345 Adams Street	Brooklyn
DCAS Trades Shop	390 Kent Avenue	Brooklyn
Brooklyn Family Court	283-289 Adams Street (330 Jay St.)	Brooklyn
Brooklyn Appellate Court	45 Monroe Place	Brooklyn
Brooklyn Civil Court	141 Livingston Street	Brooklyn
Brooklyn Criminal Court	120 Schermerhorn Street	Brooklyn
Brooklyn Supreme Court	360 Adams Street	Brooklyn
Manhattan Surrogate's Court	31 Chambers Street	Manhattan
Home Life Building	253 Broadway	Manhattan
City Planning Building	14-22 Reade Street	Manhattan
Clocktower Building	346 Broadway	Manhattan
Manhattan Supreme Court	60 Centre Street	Manhattan
Excelsior Building	137 Centre Street	Manhattan
Louis Lefkowitz Building	80 Centre Street	Manhattan
Manhattan Criminal Court	100 Centre Street	Manhattan
Manhattan Civil Court	111 Centre Street	Manhattan
100 Gold Street	100 Gold Street	Manhattan
Harlem Courthouse	170-174 E. 121st Street	Manhattan
Court Square Building	2 Lafayette Street	Manhattan
Manhattan Municipal Building	1 Centre Street	Manhattan
Medical Examiner's Building	520 First Avenue	Manhattan
Midtown Community Court	314 W. 54th Street	Manhattan
Sun Building	280 Broadway	Manhattan
Manhattan Appellate Court	27 Madison Avenue	Manhattan
Emigrant Savings Bank	49-51 Chambers Street	Manhattan
Health Building	125 Worth Street	Manhattan
Tweed Courthouse (Dept. of Education)	52 Chambers Street	Manhattan
Manhattan Family Court	60 Lafayette Street	Manhattan
City Hall	City Hall Park	Manhattan
Heckscher Building	1230 Fifth Av	Manhattan
Queens Supreme Court	88-11 Sutphin Boulevard	Queens
Queens Civil/Housing Courthouse	89-17 Sutphin Boulevard	Queens
Queens Criminal Court	125-01 Queens Boulevard	Queens
Queens Borough Hall	120-55 Queens Boulevard	Queens
Queens Family Court	89-14 Parsons Boulevard	Queens
Central Storehouse	66-26 Metropolitan Avenue	Queens
Long Island City Court	25-10 Court House Square	Queens
Staten Island Family Court	100 Richmond Terrace	Staten Island
Staten Island Village Hall	111 Canal Street	Staten Island
Staten Island Supreme Court	18 Richmond Terrace	Staten Island
Staten Island Criminal Court	67 Targee Street	Staten Island
Staten Island Civil Court	927 Castleton Avenue	Staten Island
130 Stuyvesant Place	130 Stuyvesant Place	Staten Island
Staten Island Borough Hall	10 Richmond Terrace	Staten Island



DEPARTMENT OF CITYWIDE ADMINISTRATIVE SERVICES
OFFICE OF THE COMMISSIONER

One Centre Street, 17th Floor
New York, NY 10007
(212) 669-7111 • Fax: (212) 669-8992
Email: mhirst@dcaas.nyc.gov

Martha K. Hirst
Commissioner

Citywide Personnel
Services

Facilities
Management &
Construction

Municipal Supply
Services

Real Estate Services

Citywide Equal
Employment
Opportunity

Citywide
Occupational Safety
& Health

Transportation
Services

The City Record

CityStore

April 4, 2007

Mr. John Graham
Deputy Comptroller for Audits,
Accountancy & Contracts
Office of the City Comptroller
City of New York
1 Centre Street
New York, NY 10007-2341

Re: Audit Report on the
Development and
Implementation of the
Capital Asset Management
System (CAMS) by the
Department of Citywide
Administrative Services
(7A06-112)

Dear Mr. Graham:

Thank you for the opportunity to respond to the above captioned Audit Report (the "Report") dated March 14, 2007.

After carefully reviewing the Report, we must respectfully disagree with a number of the findings and conclusions of this Audit. The decisions we have made in advancing the Capital Asset Management System (CAMS) project are rational, supportable, and in the best interest of the City of New York. In this response, we will discuss this project and the rationale for our decisions and address certain portions of the Report which we believe can be misinterpreted.

By way of background, the CAMS project arose from this agency's initiation of preliminary investigations to determine the overall condition of our portfolio of buildings and to begin to more thoroughly assess the need for Capital funding. As you know, before any City Capital monies can be spent to correct infrastructure deficiencies, a project for that work must be approved in the City Capital Budget. In order to secure project approval, a preliminary scope of work and a preliminary cost estimate for that work must be prepared. The inclusion of a project in the Capital Budget allows the City to initiate a detailed design which results in a more detailed and specific corrective action plan, detailed drawings, and a more refined cost estimate.

The result of our preliminary investigations of our buildings is CAMS, a database tool that was commissioned to facilitate planning for the rehabilitation and upgrade of DCAS-owned and -managed buildings. The overall goal of CAMS is to present a comprehensive picture of the condition of DCAS-owned and -managed buildings, so that funds are allocated and Capital work planned as systematically and cost-effectively as possible. Through the use of the information generated by CAMS, we expect to strengthen our ability to replace deteriorating infrastructure before it fails, thereby avoiding emergency repair costs, related damage to nearby areas, the corresponding loss of employee productivity, as well as potential liability on the City's part arising from potential personal injury claims.

Turning to the specifics of the Report, there are a number of misinterpretations and disagreements between the auditors and our staff concerning this project that we believe stem primarily from the following issues:

1. Although the Audit Report handles CAMS as if it were an Information Technology Project, in fact, CAMS is actually an engineering project, more than an Information System development project. Virtually all of the monies spent on this project have been in obtaining and evaluating engineering assessments concerning the condition of our buildings. The initial assessments of DCAS buildings were performed by consultant personnel who were accompanied by knowledgeable DCAS facilities and engineering employees. This data was, in turn, furnished to other DCAS architectural and engineering personnel with detailed knowledge of these buildings for their final review, discussion, potential modification, and approval.

The *smallest* part of this project involves the use of proprietary software to assist in managing this information, which is being utilized without any modification. Currently, DCAS is paying the consultant a total of \$56,400 annually, which covers the use of the proprietary software, updated releases of the software, hosting, annual updates of supporting cost-related data, and helpdesk and troubleshooting services.

2. The CAMS project is a work in progress. Although this Audit evaluated the CAMS project while still in progress, the Report fails to appropriately acknowledge that these elements are not yet complete, instead suggesting that they are simply ineffectual. Certain elements which were assessed under this Audit are still not formally in place and will not be until the project is actually completed. Thus, it was impossible for such components to be properly evaluated by your staff during this Audit.

For example, the Audit Report states that "DCAS has not formally accepted the system as being complete because the data that was collected by VFA [Vanderweil Facility Advisors] is currently under review by the Division of Facilities Management and Construction." Yet the Report also states that "we requested evidence of formal approval of the assessment data by DCAS architectural and engineering specialists", but "[w]e did not receive the supporting documentation requested."

These statements confirm that the auditors were aware that formal approvals of the information would not be available until the conclusion of the Project, yet a different section of the Report, entitled "Scope Limitation", was written in a contradictory manner that incorrectly suggests either an information quality issue or that we were not being cooperative. The fact that information concerning the final approvals of the data could not be provided because that information was still under review by appropriate DCAS staff is not a deficiency.

Similarly, the Audit concludes that "[a] Security Risk Assessment has not been performed on CAMS." In fact, we have prepared a Risk Assessment document that is currently under discussion with the City's Chief Information Security Officer (CISO) at the Department of Information Technology and Telecommunications (DoITT). That Office has advised us that our approach concerning CAMS security is not unreasonable. Once again, the fact that we are in the process of engaging in proper actions to finalize an ongoing project is not a deficiency.

3. The requirements of the data in a computer system determine the appropriate level of security for that application. The important concept is that information security is not a "one size fits all" proposition. There are some computer systems that, due to the very sensitive nature of the data that they contain, or the extremely critical nature of the system itself, will require extraordinary measures to protect that data. Conversely, there are less sensitive systems containing less sensitive information that will merit a diminished level of expense or effort to secure their information. The instant system falls within the latter category.

During the course of the Audit, we informed the auditors that we had carefully evaluated the CAMS information and had judged it to be neither sensitive, nor critical, as defined by City Comptroller Directive #18. Consistent with our evaluation of this data, we took appropriate security steps, as well as steps to ensure that the data would not be lost and could be recovered if corrupted or otherwise unavailable. This precaution entails both keeping a hard copy and electronic copies of the data on-site, in addition to the copy maintained by VFA at the ATT datacenter in Boston. Furthermore, the DCAS electronic copies of the data will also be stored on a DCAS server, which is backed-up to the DoITT datacenter, and covered under both our disaster plans. This would provide a data library that would be comprised of at least five (5) distinct copies of the data, each covering multiple time periods allowing for restoration of the data to a prior period if necessary. Therefore, even if this vendor were to fail or if its disaster plan would prove to be inadequate, we are assured that the data will be available for our use.

Contrary to our view that we need to provide appropriate security measures at the best cost, the Report suggests that we should seek out the best level of security available for this system, and "choose the vendor that will ensure optimal conditions with which to operate the system." This is apparently to be done without consideration of cost or necessity. It is our opinion that before we spend an excessive amount of time or inordinate amount of taxpayer money to bring CAMS into line with a more stringent security environment, it would be necessary to articulate the need so as to justify the additional benefits being purchased. We believe the level of security established is appropriate, justifiable, and cost-effective.

4. This Project will be completed under budget. This is a project being developed by the end-users for use by the end-users. We are utilizing existing staff to review the data and manage the project. This approach has resulted in some project delays, in part due to temporary staffing vacancies, but more importantly because all of the personnel involved need to continue to perform all of their normal job duties in addition to reviewing the condition of the entire portfolio of buildings. This has, however, also minimized overall project costs and ensured critical end-user input. We project that the completed system will be finished for less than \$2 million, a savings of \$1 million (33%) from the initial project cost estimate of \$3 million.

Such cost-savings do not occur by accident but, rather, by design. Thus, we are troubled by the statement in the Report that "scheduled periodic meetings between DCAS and VFA have not taken place since 2004," as we believe that the reader is left with the impression that the project has been languishing. As a point of clarification, we believe that such regular face-to-face meetings, which were appropriate when consultant personnel were already in New York performing surveys of the buildings, are far less efficient and desirable when the consultant personnel are not otherwise scheduled to be in New York City. Rather, we determined that beyond the initial project phase, incurring additional travel and lodging costs to hold face-to-face meetings was generally unnecessary and fiscally irresponsible. Therefore, taking advantage of modern technology, we have increasingly handled most of our meetings via telephone, email, and teleconferences, supplemented by face-to-face meetings whenever they are prudent. A cursory examination of our records indicates that additional face-to-face meetings took place on the following dates: 9/29/2005, 10/18/2005, 12/12/2005, 11/21/2005, and 8/09/2006. Teleconferences were held on: 12/14/2005, 7/06/2006, 11/20/2006 and 01/29/2007. These meetings are in addition to numerous communications between the Project Manager and the consultant by telephone and email.

There is one more comment in the Report that we believe should be clarified. In the "Scope Limitation" discussion, the Report states that "DCAS officials did not provide us with the supporting documentation needed to test the accuracy of the data in CAMS . . ." The Auditors had requested the raw data collected by the consultant personnel during their walk-through of the buildings. This statement gives the impression that we did not cooperate in this matter, which is not accurate. We did not provide this data because we do not have it.

Prior to issuing individual building reports for DCAS review and comment, the consultant, VFA, subjected the information to a quality review process. This process included validating costs by comparing them against the costs for other, similar buildings. In addition, multiple teams were used to cross-check the work of the people who visited the property. Therefore, the review of the raw data, a condition prior to the consultant's quality review, will not provide any valid indication of the accuracy of the data in CAMS. It is only the subsequent review of these judgments by other qualified personnel, as we are currently performing, that will ultimately address that issue.

Finally, to address the Report's security recommendations:

1. Immediately perform an on-site review of the VFA operations to ensure that VFA's policies and procedures comply with DOI Directives;
2. Request from VFA the primary elements of the disaster-recovery plan for the CAMS system;
3. Ensure that the disaster-recovery plan is tested in accordance with DOI Directives;

Responses 1 - 3: We believe that we have addressed these issues through the use of internal controls. Specifically, we will require VFA to provide us with a back-up of our data at regular intervals, following our major updates to this data. The backup will be stored on site at DCAS, and will be archived on our in-house server, which is, in turn, backed up to DoITT on a daily basis, and covered under their disaster plan. This procedure will provide us with copies of the data on the live VFA system at the ATT datacenter in Boston, at the VFA back-up site in Boston, and also a library of warehoused copies at DCAS and at DoITT, in addition to the hard copy data that we also have in-house.

In addition, the data will be formed into discrete capital projects and entered into the FMS Four and Ten- Year Capital Plans. FMS is housed at the FISA datacenter.

Therefore even if this data were to become corrupt due to VFA weaknesses, or if a disaster were to strike their datacenter, or if their disaster plan was found to be inadequate, we can be confident that we will not lose our data.

We will, however, follow up with the consultant regarding the testing of its disaster plan.

4. Perform an initial security-risk assessment on CAMS and then each year thereafter or when a major change to the system application is implemented;
5. Ensure adherence to applicable directives and standards identified during the security-risk assessment process; and
6. Perform a security-risk assessment on the alternate hosting site, if one is under consideration.

Responses 4 - 6: We have prepared a Risk Assessment document that is currently under discussion with the City's Chief Information Security Officer (CISO) at DoITT. We expect to finalize this shortly. If we did not host this application with VFA, the alternative would be to explore hosting at the DoITT datacenter. Since the DoITT operation is under the direction of the City's CISO, we would not perform a security Risk Assessment.

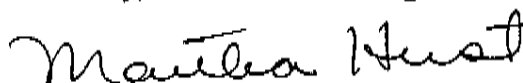
The current expectation is that we will continue the current hosting arrangement with VFA. However, we will continue to explore the security arrangements with the CISO at DoITT as well as DoITT's capability for hosting this application. Once complete we will revisit this analysis annually and update it if necessary.

7. Create a formal procedure for DCAS and VFA for the periodic review of user privileges to ensure their appropriateness and make corrections as needed.

Response 7: We will regularly review all user privileges and make changes as necessary.

Despite our differences regarding this Audit, I know that we share common goals concerning the efficient operations of City Government. I look forward to continue working with your staff toward that end.

Sincerely,



Martha K. Hirst

cc: D. Brosen
C. Lane
J. Minnier
R. Pitts
R. Tobin
M. Sarker