Nassau County
Office of the Comptroller

Limited Review of the Nassau County Department of Information Technology's Succession Planning, Hardware Inventory Control and Miscellaneous Operations

George Maragos
Comptroller

September 14, 2011

NASSAU COUNTY

OFFICE OF THE COMPTROLLER

George Maragos

Comptroller

Francis X. Moroney

Chief Deputy Comptroller

Joy M. Watson

Deputy Comptroller for Audit and Special Projects

Jostyn Hernandez

Director of Communications

Christopher Leimone

Counsel to the Comptroller

Audit Staff

JoAnn Greene

Director of Field Audit

Louis Grimaldi

Senior Project Manager

Vincent Abbatiello

Assistant Director of Field Audit

Ellen Misita

Field Audit Supervisor

Background

According to the Nassau County Charter, the Nassau County Department of Information Technology's ("IT") powers and duties include the following:

- planning, formulation and coordination of information technology and telecommunications policies for the county;
- dissemination of management information in the area of data processing and telephone communications;
- development of infrastructure and integrated systems for the use and maintenance of software applications;
- provision of assistance in providing interagency coordination on matters related to data communications and interfacing of computers;
- development, purchase and maintenance of hardware and software to meet the needs of departments of the county;
- provision of assistance to departments of the county in meeting their data processing and data communications objectives;
- planning and provision of telecommunications coordination in support of disaster recovery;
- maintenance of security for data and other information handled by all departments of county government;
- institution of procedures to assure restrictions of access to information to the appropriate individuals, where such restrictions are required by law;
- performance of such other responsibilities with respect to information technology and telecommunications matters, including responsibilities that may be delegated elsewhere by this county government law, as the County Executive may direct;
- posting of all Requests for Proposals on the official county website; and
- Commissioner of Information Technology shall supply a copy of each Request for Proposals to the Clerk of the County Legislature.[1]

2009 IT expenditures, which included telecommunication and salary costs, totaled $24,584,368 with an additional $4,506,081 encumbered. IT revenue totaled $12,774,753, which primarily represented interdepartmental revenue for services provided to other County departments. As of November 2010, revenues and expenditures were budgeted at $12,348,953 and $31,133,044, respectively.

Nassau County's 2010-2013 Capital Improvement Plan lists 43 IT capital projects with a budget of approximately $190.8 million as of November 2010.

[1] Nassau County Charter, § 2151, as updated 6/30/2010.

According to an IT Organizational Chart provided to the auditors in July 2010, the Department has a staff of 122. IT incurred approximately $11.0 million in salary costs in 2009.

Audit Scope, Objectives, and Methodology

The objective of our audit was to examine the adequacy and effectiveness of the internal controls surrounding IT's management of succession planning, hardware inventory control, and miscellaneous operations. The period audited were the years 2009 and 2010.

The audit was planned and performed to obtain reasonable assurance that the audit information is free of material misstatements. An audit includes examining documents and other available evidence that would substantiate the accuracy of the information tested, including all relevant records and contracts. It includes testing for compliance with applicable laws and regulations, and any other auditing procedures necessary to complete the examination. We believe that this audit provides a reasonable basis for the audit findings and recommendations.

Summary of Findings:

The Nassau County Department of Information Technology ("IT") Does Not Have a Succession Plan

IT has not developed a Succession Plan for the replacement of key personnel that are planning to retire or that are eligible to retire. These key employees are essential to many critical IT applications.

IT Has Not Developed a Formal Written Change Management Policy

IT does not have a formal written policy describing the change management process. This policy is essential and describes who has the authority to make changes to critical systems, and ensures that unauthorized changes and errors do not affect these systems.

IT Capital Projects Were Behind Schedule

The Comptroller's Office identified eight IT capital projects that were behind schedule.

IT Was Lacking a Complete, Current County-wide Computer Hardware Inventory

The Comptroller's Office noted that IT did not maintain a complete, current hardware inventory of all computer and peripheral equipment, thereby increasing the risk that County assets may not be safeguarded.

Password Administration Policies Are Inadequate

The software used by IT to enforce password administration policy for employee sign-on to the County network only requires that passwords change every 90 days, and does not require the use of both alpha and numeric characters.

****

The matters covered in this report have been discussed with management during the course of this audit. An Exit Conference was held with the Commissioner of IT to discuss the preliminary audit findings. IT provided a response included as an Appendix to this report.

Table of Contents

Audit Finding (1):

Need for Succession Planning to Replace Retiring Senior Programmer/Analysts

The Nassau County Department of Information Technology ("IT") does not have a succession plan for the replacement of key employees who are scheduled, or are eligible to retire in 2010. If key employees retire or leave the employment of the County, critical IT systems could be impacted because sufficient staff with knowledge to operate highly technical systems might be lacking, particularly as the County migrates to its new integrated system, Nassau Enterprise Wide System Solution ("NEWSS").

IT is staffed by key Bethpage Data Center ("BDC") operations staff and key application programmer/analysts at 240 Old Country Road, who are essential to the operation of the IT function. During our tour of the BDC, IT management informed us that key employees responsible for critical, highly technical functions are eligible for retirement. In particular, two employees responsible for maintaining the mainframe computer are currently eligible for retirement. At 240 Old Country Road, six application programmer/analysts are responsible for systems that support the following County departments: District Attorney, Correctional Center, Sheriff, Health, Police, Fire Commission, Civil Service, County Attorney and Public Works. Two of the six programmer/analysts have retired, one in August 2010 and the other in December 2010.

Considering that most of the County's key applications are out-dated and lack external programming support, it is crucial that IT develop an immediate succession plan to ensure that support for these applications continue should key employees retire.

Audit Recommendation:

IT should immediately develop a plan of succession to replace key employees with critical knowledge necessary for the support and operation of systems. The plan should include steps to hire or train staff with sufficient knowledge and experience to operate the County's critical systems.

Audit Finding (2):

Lack of a Formal Written Change Management Policy

IT did not have a formal written policy describing its change management process, which may result in unauthorized changes or programming errors being made to live production systems.

An organization's computer environment forms an integral part of the operational and support functions of an organization. Consequently, any change to the current applications will affect the organization's business operations. Therefore, it is critical to minimize the adverse effect of changes made to programs or data and facilitate the operation of the business. For this reason, changes to application programs and data are performed in a test area so that production programs and data are not affected by changes until changes have been tested, reviewed by supervisors and approved by supervisors before being implemented into production. This method prevents business processes from being affected by changes that may be incorrect or unauthorized.

This process is normally documented in a formal, written policy that describes who is authorized to make changes, review changes and approve changes for movement to the production environment where actual programs run. The policy should indicate the type and level of access granted to programmers who perform testing and those programmers who move programs to the production environment. The policy should also indicate which programmers are authorized to move programs to the production environment. Documentation should be maintained indicating who made changes, when changes were made and who reviewed and approved changes.

Due to its lack of a formal written policy describing the change management process, changes are made based upon application problems as they arise, e-mail requests for changes, changes required by union contract agreements including Memorandums of Agreement and Stipulations, County Ordinances and changes required by external entities that send or receive data to/from the mainframe. In addition, changes are made directly to production programs rather than in a test environment.

The risk of changes containing errors and adversely affecting production programs and the associated business processes is increased due to the lack of an appropriate change review and approval process. The risk of unauthorized changes and errors made to production programs or data is also increased.

Audit Recommendation:

IT should:

a) develop a formal written change management policy. The policy should indicate the level of access granted to programmers. It should indicate who is authorized to make changes, review changes, approve changes and move changes to the production environment from the test environment. It should also specify the nature of documentation required to identify who made changes and when changes were made, reviewed, approved and moved to production. Documentation should be maintained for audit purposes; and

b) implement procedures to ensure that all authorized changes to applications are first made in a test environment and then moved to the production environment only after successful completion of adequate testing of the changes.

Audit Finding (3):

IT Capital Projects Were Behind Schedule

As of November 2010, the Nassau County 2010-2013 Capital Improvement Plan lists 43 technology capital projects with a total multi-year budget of $190.8 million. We obtained a list of capital projects from IT, which listed the completion status of the projects. We determined that 22 capital projects listed in the County's Capital Improvement Plan were not included in the list of capital projects provided to the auditors by IT. In addition, the following eight projects on IT's list were past their respective completion dates:

Project 97116, Sheriff's Accounting System, 47% complete;

Project 97117, CAMDR, 54% complete;

Project 97120, Data Center Storage, 55% complete;

Project 97122, Microsoft Office Sharepoint Server, 39% complete;

Project 97128, Treasurer's Paperless Check System, 6% complete;

Project 97130, OSCAR, 0% complete;

Project 97133, Sharepoint/Project Server Infrastructure, 1% complete; and,

Project 97590, Update Fire Marshal Fee Collection System, 67% complete.

We had requested more information regarding the status of these projects, however, to-date, IT has not responded to our requests.

Audit Recommendation:

IT management should:

a) determine the causes of the projects' delays and address the issues with a Strategic Planning Committee that should be overseeing the technology capital projects. If a Committee does not exist, then the issues should be addressed with Senior County Management and the Capital Improvement Plan should be revisited accordingly; and

b) ensure that its records are complete with respect to all capital projects to ensure adequate oversight of the progress of outstanding projects.

Audit Finding (4):

Lack of a Countywide Computer Hardware Inventory

Our review noted that IT did not maintain a complete, current hardware inventory of all computer and peripheral equipment, thereby increasing the risk that County assets may not be safeguarded.

IT has established policies for the management of computer hardware, entitled: *IT Asset Management Program, Asset Management Implementation Instructions*, and *Equipment Replacement Program*. However, we did not find evidence that these policies were implemented.

In 2009 and 2008, computer hardware purchases by the County amounted to $1.3 million and $1.2 million, respectively.

In order to maintain control over the custody and location of computer equipment, information technology departments typically maintain an accurate and current inventory of all computer hardware. The inventory usually lists a brief description of the hardware, the cost of the hardware, the acquisition date, the model number, serial number, and building and room location of the hardware, and to whom the hardware was issued.

Although the County's official inventory record is the Fixed Asset Accounting Control System ("FAACS"), IT is responsible for the purchase, installation and removal of all computer and peripheral equipment. Based on past practice, IT has been responsible for entering all County computer equipment it purchased on behalf of each department into FAACS. Without a separate inventory maintained by IT and updated on a continual basis, the accuracy of FAACS may be compromised and IT may not know the location or be able to verify the existence of the hardware.

Audit Recommendation:

In order to maintain control of the inventory and to support periodic physical inventories of the equipment, IT should maintain a separate hardware inventory of all computer equipment and peripherals beginning as of the date of purchase. This inventory should be used by IT to update FAACS and should be periodically reconciled to FAACS by IT and the respective County Departments to which the equipment was issued.

Audit Finding (5):

Password Administration Policies are Inadequate

Computer systems normally contain software that enforces certain password administration standards. These standards usually require that passwords be changed after a specified period of time or number of uses, be a minimum length of eight characters or more, at least one character from each of these categories: alpha, numeric and special characters, limit the number of incorrect passwords entered, and deactivate passwords after an extended period of inactivity.[2]

[2] Document provided by IT under Security, Best Practices, "Practices for Protecting Information Resources Assets", pages 3.26 and 3.27.

The software used by IT to enforce password administration policy for employee sign-on to the County network only requires that passwords change every 90 days.[3] The software does not enforce password complexity by requiring both alpha and numeric characters. It does not limit the number of incorrect passwords, or deactivate passwords after an extended period of inactivity.

By not enforcing these password standards, the risk of unauthorized access to the County network increases.

Audit Recommendations:

IT should modify the software used to enforce password administration standards to require the following:

a) employee passwords be changed every 30-60 days;

b) passwords contain both alpha and numeric characters;

c) limit the number of incorrect passwords entered; and

d) deactivate passwords after an extended period of inactivity.

[3] D & T Nassau County “Report to Management”, year ended December 31, 2009, p.11 recommends 30-60 days.

Limited Review of Nassau County's IT Succession Planning, Hardware Inventory Control and Miscellaneous Planning
May 17, 2011

I. SUMMARY.

The Limited Review of the Nassau County Department of Information Technology's Succession Planning, Hardware Inventory Control and Miscellaneous Operations resulted in five (5) recommendations, which we have addressed below. We have accepted all five and have noted our proposed remedial actions.

II. COMPTROLLER'S OFFICE RECOMMENDATIONS.

Audit Finding (1): Need for Succession Planning to Replace Retiring Senior Programmer/Analysts

Audit Recommendation: IT should immediately develop a plan of succession to replace key employees with critical knowledge necessary for the support and operation of systems. The plan should include steps to hire or train staff with sufficient knowledge and experience to operate the County's critical systems.

IT Response: Agree. IT will develop a two-phased plan to address: (1) replacement of those identified employees who are near-term retirement candidates, and (2) broader issues of succession that relate to our long term ability to support systems under development. Hiring justification will be presented to the Administration, and job descriptions will be reviewed with HR and Civil Service.

Audit Finding (2): Lack of a Formal Written Change Management Policy

Audit Recommendation: IT should:

a. Develop a formal written change management policy. The policy should indicate the level of access granted to programmers. It should indicate who is authorized to make changes, review changes, approve changes and move changes to the production environment from the test environment. It should also specify the nature of documentation required to identify who made changes and when changes were made, reviewed, approved and moved to production. Documentation should be maintained for audit purposes; and

b. Implement procedures to ensure that all authorized changes to applications are first made in a test environment and then moved to the production environment only after successful completion of adequate testing of the changes.

IT Response: Agree. IT will develop and issue a formal Change Management Policy, accompanied by the process/procedures to be followed to implement the policy. The latter will include periodic audits to ensure compliance.

The production turnover process will be reviewed and strengthened, to add the necessary testing disciplines and signoffs. This effort will include a review, and upgrade where necessary, of the Staging and Test environments.

Audit Finding (3): IT Capital Projects Were Behind Schedule.
Audit Recommendation:

IT management should:

a. Determine the causes of the projects' delays and address the issues with a Strategic Planning Committee that should be overseeing the technology capital projects. If a Committee does not exist, then the issues should be addressed with Senior County Management and the Capital Improvement Plan should be revisited accordingly; and

b. Ensure that its records are complete with respect to all capital projects to ensure adequate oversight of the progress of outstanding projects.

Response: Agree. In the absence of a Strategic Planning Committee, we will recommend nominees for a senior management Steering Committee which, once formed, will review status of all projects on a periodic basis. Initial focus will be on project slippage, and on available resources vs. project commitments.

The Project Management Office will review and refresh project plans and schedules.

Audit Finding (4): Lack of a Countywide Computer Hardware Inventory.
Audit Recommendation: In order to maintain control of the inventory and to support periodic physical inventories of the equipment, IT should maintain a separate hardware inventory of all computer equipment and peripherals beginning as of the date of purchase. This inventory should be used by IT to update FAACS and should be periodically reconciled to FAACS by IT and the respective County Departments to which the equipment was issued.

IT Response: Agree. IT will revisit the installed equipment in the Bethpage, HHS, and PD facilities and develop a comprehensive County-wide computer inventory. Much of the information is available in multiple documents and surveys, and can be assembled without starting from scratch. Once assembled, we will update FAACS, and implement a procedure for periodic updates.

Audit Finding (5): Password Administration Policies are Inadequate.
Audit Recommendation:
IT should modify the software used to enforce password administration standards to require the following:

a. employee passwords be changed every 30-60 days;

b. passwords contain both alpha and numeric characters;

c. limit the number of incorrect passwords entered; and

d. deactivate passwords after an extended period of inactivity

IT Response: Agree. We will alter the timing for changes, the makeup of each password, the number of errors accepted, and the deactivation timing. We will prioritize the various access portals, to address higher risk items first, as we apply scarce resources to effect the changes.

IV. RESOURCE REQUIREMENTS.

At the time of the Audit, the staffing level for Information Technology was **122,** as noted in the Draft Report. Since that time, the Data Entry staff at HHS has been transferred from IT to DSS, and several people have retired, resulting in a staff count of **92.**

The department has launched an infrastructure Performance Improvement Program, to address the audit points cited above, as well as the disaster recovery and network issues cited earlier. Once again, we will prioritize, based on resource availability.

Auditors' Follow-up Response:

We concur with IT's plan of action to address the recommendations of the Comptroller's Office, and stress the importance of acting promptly in implementing all of the recommendations.