Department of Community Affairs
Information Technology Controls

September 15, 2003 to June 30, 2004
The Honorable Richard J. Codey  
Acting Governor of New Jersey  

The Honorable Richard J. Codey  
President of the Senate  

The Honorable Albio Sires  
Speaker of the General Assembly  

Mr. Albert Porroni  
Executive Director  
Office of Legislative Services  

Enclosed is our report on the audit of the Department of Community Affairs, Information Technology Controls for the period September 15, 2003 to June 30, 2004. If you would like a personal briefing, please call me at (609) 292-3700.

December 1, 2004
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>1</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>IT Strategic Plan</td>
<td>4</td>
</tr>
<tr>
<td>System Documentation and Administration</td>
<td>5</td>
</tr>
<tr>
<td>System Security</td>
<td>6</td>
</tr>
<tr>
<td>Test Environment</td>
<td>8</td>
</tr>
</tbody>
</table>
Department of Community Affairs
Information Technology Controls

Scope

We have completed an audit of the Department of Community Affairs, Information Technology Controls for the period September 15, 2003 through June 30, 2004. We assessed network vulnerability and reviewed the adequacy of information technology (IT) policies and procedures. Our audit evaluated the following selected aspects of the controls in place over the department’s network and systems that process and protect both public and private information.

• IT strategic planning.

• Documentation of the system and changes over hardware and application software.

• Protection of department resources from unauthorized access, use, and alteration; and physical and logical security in place to protect the department’s IT infrastructure.

• Business continuity plans in the event of processing interruptions.

Objectives

The objectives of our audit were to determine the adequacy of security controls over the computer network to minimize the risk of unauthorized physical or logical access, and to review the adequacy of management planning for IT operations.

This audit was conducted pursuant to the State Auditor’s responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with Governmental Auditing Standards issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by the Open Source Security Testing Methodology
Manual provided by the Institute for Security and Open Methodologies, and the Gold Standard Benchmarks issued by the Center for Internet Security.

In preparation for our testing, we studied legislation, agency operation plans, procedural guidelines and flow charts, and industry and governmental standards for computer security and operation. Provisions that we considered significant were documented and compliance with those standards was verified by interview of key personnel, observation, and access of network infrastructure, and through other tests we considered necessary.

A nonstatistical sampling approach was used. Our samples were designed to provide conclusions about internal control attributes. Sample items were selected judgmentally.

Conclusion

The Department of Community Affairs’ (DCA) management has recognized the importance of security over the department’s network and the services it provides. However, we have found several internal control weaknesses within the security controls effort. We also noted a lack of effective IT strategic planning.

We have also provided DCA with a management letter containing a more detailed discussion of network security specifics.

Overview

The DCA network contains 49 servers that house various applications and databases, as well as approximately 866 workstations. The network houses both public and private information. One critical application collects and records data from the field offices for the federal Section 8 housing program. The data collected is stored in a database on a database server physically located in the server room in the DCA building. The database is sent to the federal Department of Housing and Urban Development on a monthly basis.
In October 2003, the network was experiencing outages, the email service was not dependable, and there were connectivity problems. Presently, the network is running with minimal problems. It is our understanding that previous configuration and implementation errors during a network upgrade had contributed to the difficulties experienced early in the process. A vendor had been hired by prior management in April 2000 to assist in the design and implementation of the network upgrade from an outdated environment. The vendor subsequently went bankrupt in June 2000 leaving the department with a partially designed and installed network environment. A commitment was then made to migrate to a more current server environment. At that time, the Commissioner instructed the IT unit to do what was needed to complete the network quickly. Between May and August 2003, configuration and implementation errors contributed to the difficulties. The configuration errors and implementation mistakes were slowly corrected and fixed over the next five months. Additional equipment was purchased to complete the network upgrade from January to March 2004. Presently, the network is running with minimal difficulty.

Following are the weaknesses that still need to be addressed.
The department’s Information Technology Strategic Plan (ITSP) is not current.

The department of Community Affairs has an ITSP identifying IT related projects. The plan is dated July 31, 2000, and was based on “ten priority goals appropriate to the Department’s business needs over the next three to five years”. However, the plan has not been reviewed and updated to include initiatives undertaken since July 31, 2000, changes in objectives and technology, and the status of previous projects.

The National Association of State Chief Information Officers, in their Enterprise Architecture Development Tool Kit, states that the ITSP is an evolving document that should be reviewed and updated on a regular basis to meet the demands of the organization.

Additionally, the Control Objectives for Information Technology (CoBiT), Defining a Strategic Information Technology Plan, Control Objective 1.5 - Short Range Planning for the IT Function, states that senior management should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions.

**Recommendation**

The department should review the current business plan and goals and update the master ITSP where necessary. The ITSP should also be updated for previous objectives and strategies completed or in process.

**Auditee Response**

The department has formed an IT executive Steering Committee that addresses consistency in IT planning, but the formal plan dated July 31, 2000 has not been updated. Based on limited staffing resources, this activity will not take priority at this time.
The network has not been properly documented, making it difficult to control changes and upgrades.

System Documentation and Administration

Network Documentation

Network schematics provide an agency with an inventory of servers and users’ workstations via network addresses. A catalog of servers and workstations provides an agency with an inventory of their hardware, services, applications, and users. CoBiT’s - Planning and Organization Control Objective 2.1 - Define the Information Architecture states: “Information should be kept consistent with needs and should be identified, captured and communicated in a form and time frame that enables people to carry out their responsibilities effectively and on a timely basis. Accordingly, the IT function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the IT long-range plan.”

Our review found minimal documentation in the form of network schematics and network catalogs. This creates access and system vulnerabilities for DCA since they do not have a complete inventory of hardware, applications, services and users on agency servers and workstations.

Three employees are responsible for DCA’s network administration tasks, which is an insufficient number of staff for the daily responsibilities of network maintenance, change management of server and application upgrades, and assistance to DCA’s Help Desk and individual DCA users.

Change Management

A strong system of internal control over hardware and software changes mandates that changes be documented in order to create an adequate change
history. We noted that a policy was developed in April 2004 but not implemented.

Recommendation

We recommend that the department create a network schematic and a network catalog of hardware, applications, and users, using network diagraming software and administrator tools. In addition, DCA should implement their change management policy. Finally, DCA should hire additional network staff for the important maintenance and security functions.

Auditee Response

DCA will investigate the use of the network diagraming tools as recommended in this audit. Implementation is expected during the summer of 2005.

DCA agrees that the staffing currently in place in the network area is insufficient, but the ability to increase staff at this time is hindered by budget limitations.

System Security

Network Security

A comprehensive network security program encompasses several pieces that must be properly managed. These include firewalls, switches and routers, physical access points, anti-virus and intrusion detection software, and e-mail and messaging software access. If these components are not properly secured, the risks of service disruption and exposure of confidential data are increased.

DCA management of security for these network components should be improved. We have provided DCA with technical details to allow them to address these issues.
Network Access

Adequate control over a network requires proper administration of passwords and user accounts, compliance with accepted technical standards, and the granting of access privileges based on need. DCA should strengthen controls over these areas, and we have provided management with the technical details on these matters.

Network Services

The DCA network allows services over connections between computers that are not necessary. Allowing these services increases the risk of unauthorized access and network disruption.

These services should be shut down, and we have provided DCA with the necessary technical details.

Public Information

Care must be taken in exposing information to the public that could pose a security risk. DCA should strengthen policies and practices in this area, and we have provided them the specifics of what we found.

Network Administration

Strong network administration requires the recording and monitoring of activity and the timely updating of network software. DCA should take additional steps in these areas, and we have provided management with the details necessary to do so.

Recommendation

To strengthen system security we recommend DCA

- Take the appropriate steps to strengthen the security of the network.
- Take steps to ensure network access is properly controlled.
• Have network administrators turn off unnecessary services and regularly monitor the network to ensure none are improperly enabled in the future.

• Ensure management establish and promulgate policies regarding the exposure of information, and regularly monitor what is provided to the public.

• Take appropriate steps to strengthen network administration.

**Auditee Response**

The DCA Network group has plans in place to continue to strengthen network security. This includes additional software to control access and additional use of features available in currently installed software. This software activity is expected to be complete by the summer of 2005. Plans are also being developed to improve daily monitoring of network activity and public information regarding upgrades for improved control. Daily monitoring will depend upon the availability of resources.

---

**Test Environment**

A properly designed and planned network infrastructure should include a test environment separate from the production environment in order to safely test the effectiveness of patches and upgrades. The department does not have a test environment separate from production to test patches and upgrades prior to installation on production machines. Currently, all patches and upgrades are made directly to production machines, sometimes without testing. As a result, vendor patches and/or upgrades could crash a server or application requiring them to be reinstalled and/or reconfigured. We also noted that vendor websites are often not reviewed for update release notes that may have a negative impact when installing a patch or upgrade.
**Recommendation**

We recommend that the department plan, design, and implement a test environment that would mirror the production environment. This would allow them to sufficiently test any patches or upgrades prior to installation to production machines. We also recommend that network technicians thoroughly research patches and upgrades for known problems on vendor websites.

**Auditee Response**

The DCA Network group is planning for a test network that will help to minimize the impact of change on the production network. This will be worked on over the next 18 months as equipment and resources become available.