**CITY OF DALLAS**

**Dallas City Council**

**Mayor**
Tom Leppert

**Mayor Pro Tem**
Dr. Elba Garcia

**Deputy Mayor Pro Tem**
Dwaine Caraway

**Council Members**
Jerry Allen
Tennell Atkins
Carolyn Davis
Angela Hunt
Vonciel Jones Hill
Sheffield Kadane
Linda Koop
Pauline Medrano
Ron Natinsky
Dave Neumann
Mitchell Rasansky
Steve Salazar

**Office of the City Auditor**

**Audit Report**

# AUDIT OF THE SERVICE LEVEL AGREEMENT OF THE at&t MANAGED SERVICES AGREEMENT

(Report No. A07-019)

**September 28, 2007**

**City Auditor**

Craig D. Kinton

# Table of Contents

## Executive Summary

This report identifies the continued lack of effective contract management by City staff and inadequate performance by our vendor, **at&t**. A previous audit[1], performed between September and December 2006 (issued March 2007), identified that sufficient data did not exist, nor were processes in place, to substantiate compliance with all of the terms and conditions of the contract. Although **at&t** is now maintaining data on services delivered to the City, **at&t** has not instituted all processes necessary to substantiate compliance. **Of particular concern, this audit identified evidence of serious lapses of procedures to ensure the security of the City's network.**

**at&t's** performance in providing security services as specified in the contract was sub-standard. Forty security compliance tests were performed. The results of these tests were:

- Signature Updates (27 tests) – 20 Failed;
- Critical Event Notification (four tests) – All failed;
- Firewall Configuration Backup (six tests) – All failed;
- Bandwidth Utilization (one test) – Failed;
- Real-Time Intrusion Detection (one test) – Passed; and,
- Debugging Level Logs (one test) – Passed

**at&t's** performance in providing network management services improved, but Fault Event reporting processes need enhancement. Data was not on the Fault Event Report which identified the devices monitored and reported. Without this information, it impairs the City's ability to determine what devices are not meeting service level agreements.

The audit objective was to determine if **at&t** is complying with the terms and conditions of the seven-year, $59,984,714 Managed Services Agreement. This agreement provides for the management and monitoring of the City's voice and data network as specified in the Service Level Agreement (SLA). The SLA metrics specify penalties, up to and including termination, if **at&t** fails to meet the performance requirements.

[1] Audit conducted under authority of Dallas City Charter, Chapter IX, Section 3.

## Recommendations Summary

We recommend that the Director of Communication and Information Services (CIS):

**Recommendation 1:**

- Ensure that **at&t** implements policies and procedures designed to fulfill all contract deliverables, especially those related to security, and provide sufficient data for CIS to monitor and determine contract compliance.

- Consult with the City Attorney and take appropriate action to recover fees paid to **at&t** for their violation of the contract provisions governing security operations performed at the Dublin, California site.

**Recommendation 2:**

- Remove **at&t's** sub-contractors from contract monitoring responsibilities.
- Designate specific personnel to continually monitor and test for compliance with the terms and conditions of the **at&t** contract. These personnel should:
    a. Maintain documentation of the tests performed;
    b. Evaluate the test results; and,
    c. Compare test results against contract requirements.

## Management's Response Summary

**Recommendation 1:**

- The CIS Department and **at&t** have implemented the policies and procedures necessary to fulfill all security contractual deliverables. The implementation of these policies and procedures removes any concerns of security failures.

- **at&t** has agreed to credit the City of Dallas **$24,987.00**. This credit is based on the nine months the contact was not compliant and **at&t** added an additional five months of credits.

**Recommendation 2:**

- CIS has implemented organizational changes to ensure that the **at&t** contract is properly monitored and in contract compliance. The Director/CIO of CIS has reorganized the organization and implemented a Contract Compliance / Contract Administration team to the **at&t** contract.

## Audit Results

### I. at&t continues to violate contract terms and conditions and CIS is not detecting and requiring corrective action of these violations.

Significant contract violations still remain, particularly in the area of network security. The inability of the **at&t** systems to capture all security events is indicative of systemic technical and procedural problems. Although performance criteria are established in the SLAs, the failure of **at&t** performance monitoring systems to identify and report some of the more significant security events undermines confidence in the reliability of their contract performance reporting systems. SLA performance parameters are to ensure reliable and consistent protection of the City's voice and data network.

The March 2007 audit identified policies and procedures that **at&t** should have implemented to ensure that all contract deliverable requirements were defined and that the SLA compliance methodology was developed and implemented. Although we briefed **at&t** and CIS on contract compliance concerns prior to the release of the audit on March 16, 2007, it appears that the policies and procedures were developed by **at&t** shortly before our arrival for this audit. A review of the procedural documentation provided to us shows a date of April 27, 2007, six days before the commencement of the onsite work. Further, the procedures developed by **at&t** were incomplete as evidenced by the omission of required notifications.

To help ensure that **at&t** understood and could document evidence supporting contract compliance, assistance was provided by CIS and the City Auditor's Office to address previous contract compliance deficiencies identified during the September 2006 site visit in Dublin, California.

The results of the May 2007 audit tests show a continued gap in service delivery which is discussed below:

- ***Security***
  - *Intrusion Detection System (IDS) Signature Updates* –

    **at&t** did not timely install 20 of 27 (74%) of the test sample signature updates to the IDS. Further, **at&t** allowed the IDS software license to lapse for a period of time, leaving the City's network vulnerable to the exploits addressed by the signature updates. The loss of protection during this period is a critical event. An IDS system detects attacks on a network. The manufacturer of the IDS system regularly publishes updates to

the system that provide additional threat identification capability. These updates are called "signature updates."

- *Critical Event Notification –*

  Of the four tests conducted, it was discovered that **at&t** did not report any of the critical events within the 15-minute timeframe required under the contract. A critical event is any event that can negatively affect the performance and security of the network. The tests that failed included a failure to validate a privileged system login, an HTTP vulnerability, an authorization failure, and a DNS leak. Although **at&t** and CIS worked together since the March 2007 audit to define the eight events that are to be considered "critical", **at&t's** security reporting systems continue to be deficient. The four tests failed because **at&t** did not notify the City within 15 minutes of the occurrence of the event. The actual time it took **at&t** to report these events to the City ranged from approximately 33 minutes to over six hours.

- *IDS License Expiration –*

  **at&t** failed to notify the City that the license for the IDS security device had lapsed during the latter part of 2006. Because of this lack of communication and the failure of the **at&t** systems to record and report the event to the City, there are no assurances that **at&t**'s systems are sufficiently equipped to report all security events. This reporting capability is the foundational component for determining **at&t**'s compliance with the SLA. Without the assurance that all security events are monitored, recorded, and reported, the measurement of **at&t**'s performance against the SLAs is indeterminable.

- *Backups of Firewall Configuration After Firewall Change –*

  Of the six firewall changes tested, four (66%) did not initiate a backup of the firewall. The two backups that were performed were greater than the two hour timeframe allowed in the contract; therefore, 100% of the sample tested was not in compliance with the contract. Timely backups of the firewall configuration are important to the security of the network because in the case of a firewall failure, the most up-to-date security rules would be available for rapid re-installation to prevent unauthorized entry into the City's network.

- *Bandwidth Utilization –*

  This test failed because only a summary of bandwidth utilization was provided that relates to a single point in time, in lieu of measuring bandwidth utilization over an extended period of

time. In addition, there is a question as to the accuracy of the snapshot report based upon a software issue where connection ID values may have negative numbers. The bandwidth utilization report is important because it reports performance degradation within the City's network over time and provides the technical support team a starting point in isolating the cause of the degradation.

Due to the significant number of security requirements found to be non-compliant, we believe that **at&t** has been paid for substandard service delivery. The security component of the contract covers 12 service categories with SLAs for each category. The City is paying $3,571 per month for these services. The remedy cited in the contract if **at&t** fails to meet the service performance requirements of the SLAs is that the City may terminate the contract at its sole discretion.

- ***Network Management and Service Level Agreement***

Data was not on a Fault Event report which identified the devices monitored and reported. Without this information, CIS is unable to determine what devices are not meeting SLAs.

- ***Service Level Agreement for Equipment and Telephony Services***

**at&t** and CIS have worked to develop an accurate listing of the number of sites per Site Type as defined in the contract. According to CIS, the list and classification of City locations into Site Types are now accurately established. The number of sites per Site Type was determined prior to commencement of the contract in August 2004. The contract defines 247 sites classified into six different Site Types. The revised Site Types and number of sites agreed to by CIS and **at&t** are shown below:

| Site Type | Sites Count Per Contract | Revised Site Count |
|---|---|---|
| 1 | 75 | 78 |
| 2 | 43 | 43 |
| 3 | 111 | 129 |
| 4 | 18 | 38 |
| **Total** | **247** | **288** |

- ***Record Retention***

  The types of records that must be retained are now defined in the agreement between the City and **at&t** dated April 2007.

**Recommendation 1:**

We recommend that the Director of CIS:

- Ensure that **at&t** implements policies and procedures designed to fulfill all contract deliverables, especially those related to security, and provide sufficient data for CIS to monitor and determine contract compliance.

- Consult with the City Attorney and take appropriate action to recover fees paid to **at&t** for their violation of the contract provisions governing security operations performed at the Dublin, California site.

**Management's Response**

- The CIS Department and **at&t** have implemented the policies and procedures necessary to fulfill all security contractual deliverables. The implementation of these policies and procedures takes care of the contractual network security violations and vulnerability. Network security policies and procedures have been implemented in the areas of:

  - Intrusion Detection System (IDS) Signature Updates (implemented April 22, 2007);
  - Critical Event Notification (implemented May 2007);
  - IDS License Renewal (installed April 26, 2007); and,
  - Procedures for Back Ups of Firewall Configuration Firewall Changes (implemented April 27, 2007)

  **at&t** has implemented data capturing procedures to provide CIS with sufficient data to monitor results. These data capturing procedures provide reports to CIS in the areas of:

  - Bandwidth Utilization**;**
  - Network Management and Service Level Agreement;
  - Equipment and Telephony Services; and,
  - Record Retention.

- **at&t** has agreed to credit the City of Dallas **$24,987.00**. This credit is based on the nine months the contact is not compliant and **at&t** added an additional five months of credits.

## II. CIS monitoring of the at&t contract continues to be inadequate.

Although the previous audit (March 2007) recommended that CIS ensure that **at&t** implements policies and procedures to provide the defined contract deliverables, it was apparent from our fieldwork that **at&t** had not developed adequate policies and procedures to ensure compliance with the contract terms and conditions. Between March and May 2007, CIS only developed nominal steps to improve the contract monitoring of **at&t**. This lack of contract monitoring resulted in the City not noticing that performance of significant contract terms and conditions was deficient. The failure to meet contract terms and conditions by **at&t** resulted in the serious and unnecessary exposure of the City's network and systems to security threats.

The causes of inadequate contract monitoring by CIS include:

- ***Responsibilities for monitoring / administering the at&t contract within CIS were not clearly defined.***

  Requirements analysis needs to be performed by CIS to determine the time and resources necessary to perform adequate monitoring and testing of the **at&t** contract.

  When CIS personnel were interviewed, they were unclear as to who was responsible for monitoring what parts of the **at&t** contract - the contract administrator or the security and network managers. Some of the elements that caused confusion include:

  - A new contract administrator was designated in April 2007, but during the audit period the administrator did not become actively involved in reviewing the contract deliverables that were supposed to be provided by **at&t**.
  - CIS relied upon the assistance of the former security manager even though he began providing support in another area of CIS.
  - The current security manager is now a contractor from Orion Communications, a sub-contractor of **at&t**. The contractor was assigned along with the former security manager to support the audit effort at Dublin, California. The appropriateness of having a sub-contractor in the position of monitoring the effectiveness of the vendor for whom he is working is questionable.

- The former network manager has also transitioned to another position; however, he retains responsibility to monitor the contract.

o ***Inadequate documentation of tests performed.***

CIS did not have or produce any substantive data of the tests or the results of the tests performed in February 2007. CIS personnel traveled to Dublin, California to review the status of contract terms and conditions that were out of compliance based upon the audit work conducted in September 2006. In April 2007, the City Auditor met with CIS and **at&t** to discuss the upcoming audit and the tests to be performed. **at&t** and CIS personnel indicated that **at&t** was meeting their contract requirements and was sufficiently prepared to undergo a new audit; however, it is apparent from the May 2007 test results cited in Audit Result I, that the work performed by CIS personnel was deficient.

To ensure that the City is receiving all services due, contract performance by **at&t** must be at or above the terms and conditions specified in the contract. Contract performance must therefore be adequately monitored, tested, and documented by CIS.

**Recommendation 2:**

We recommend that the Director of CIS:

- Remove **at&t's** sub-contractors from contract monitoring responsibilities.
- Designate specific personnel to continually monitor and test for compliance with the terms and conditions of the **at&t** contract. These personnel should:
    a. Maintain documentation of the tests performed;
    b. Evaluate the test results; and,
    c. Compare test results against contract requirements.

**Management's Response**

CIS has implemented organizational changes to ensure that the **at&t** contract is properly monitored and in contract compliance. The Director/CIO of CIS has reorganized the organization and implemented a Contract Compliance /

Contract Administration team to the **at&t** contract. The Contract Compliance / Contract administration team will:

- Maintain documentation of the tests performed;
- Evaluate the test results; and,
- Compare test results against contract requirements

# Appendix I

## Background, Objective, Scope and Methodology

### Background

On August 25, 2004, the City signed a seven-year, $59,984,714 Managed Services Agreement with SBC that transferred full responsibility for the provision, delivery, installation, and maintenance of all equipment, software, and services for the majority of the City's network to SBC (hereinafter referred to as **at&t**). The contract is a comprehensive agreement designed to provide the City with telephone services, network data services, and equipment. **at&t** assumed direct responsibility for services and equipment related to the operation of the City's network. The primary areas covered by the agreement include:

| Service | Description |
|---|---|
| VoIP (Voice over Internet Protocol) | Allows use of the City's data network to make local and long distance telephone calls |
| Software and Software licenses | Includes software and licenses for the following systems:<br>• Cisco Emergency Responder – identifies originating location of a 9-1-1 VoIP call placed within City facilities<br>• Asset Management – Software/licenses for asset management system, servers, and back-up software<br>• Un-Provisioned Sites – Software/licenses for Cisco routers/switches used to connect 75 un-provisioned sites<br>*Note: An un-provisioned site is a site that was not included in the original implementation. Examples include library or fire stations not yet built.* |
| Managed Services | Includes:<br>• Consulting and Engineering<br>• Help Desk<br>• Un-Provisioned Sites<br>• Asset Management<br>• Moves, Adds, Changes of Telephone Equipment<br>• Network Monitoring/Management<br>• Maintenance<br>• Cisco Emergency Responder<br>• Security |
| Telephony Services | Local and long distance telephone service |

The original timeline included in the contract provided that the majority of the implementation work was to be completed by the end of 2004. The Cisco Emergency Responder and Electronic Billing systems were scheduled for completion in June and October 2005, respectively. **at&t** and the City agreed that the timeline as presented in the contract did not accurately reflect the

amount of time required to complete the tasks so they jointly revised the due dates in many of the key operational areas. The due dates were extended and reflected a fully implemented and operational system beginning December 2005. These key operational areas included:

- Network Assessment;
- Vulnerability Assessment;
- Network Monitoring;
- Perimeter Security and Intrusion Detection;
- Cisco Emergency Responder; and,
- Asset Management System

As the implementation continued, delays of up to 24 months from the original timeline were experienced in some areas. For example, Security Intrusion and Detection was originally scheduled to be operational in September 2004, but was not fully operational until September 2006.

The Communications Division of CIS was assigned responsibility for managing the project implementation and ensuring that **at&t** was complying with the terms and conditions of the contract. One Assistant Director and two managers from the division were responsible for contract administration.

Section 38k of the agreement gives the City the right to execute a performance audit at any time with no frequency limitations and the right to perform a billing audit once per year. In the spring of 2006, the City Auditor's Office notified **at&t** of their intent to audit the agreement. The agreement contains over 200 specific deliverables that **at&t** is to achieve on a daily, weekly, monthly, or one-time basis. These deliverables formed the basis of the first audit.

On March 16, 2007, the City Auditor's Office released an audit entitled, "Audit of the Service Level Agreement of the SBC DataComm Managed Services Agreement." The audit reported the results of on-site fieldwork performed at the **at&t** Security Operations Center in Dublin, California. Not all audit tests were completed during the onsite visit to Dublin. As a result of the March 16, 2007 audit results and failure of a significant portion of the security tests, it was determined that a second audit was needed. The second audit (this audit) began with an onsite re-visit to Dublin, California on May 3 and 4, 2007.

## Objectives, Scope and Methodology

The audit objective was to determine if **at&t** is complying with the terms and conditions of the Service Level Agreement as found in the **at&t** DataComm Managed Services Agreement.

The audit was conducted in accordance with generally accepted government auditing standards and covered the period of September 2006 through May 2007; however, any related records, procedures, and events occurring before and after this period were reviewed.

To develop an understanding of relevant internal controls and controls within **at&t** and the City, managers and staff from CIS, **at&t** project managers, and **at&t** operations representatives were interviewed.

Tests that had failed during the September 2006 site visit were repeated and tests were performed that were not executed as part of the September 2006 site visit. The same individual test scripts as used previously in September 2006 were used again. The scripts specified the methodology of the tests and also included a review of internal controls pertinent to the execution of the scripts. CIS management was interviewed to determine what steps had been taken since the September 2006 site visit to ensure contract compliance. The repeat tests were conducted at **at&t's** Security Operations Center located in Dublin, California. Interviews were held in Dublin, California and at City facilities in Dallas, Texas.

## Appendix II

## Major Contributors to this Report

Paul T. Garner, Assistant City Auditor
Tony Aguilar, CISA, Project Manager
Theresa Hampden, Quality Control Manager

## Appendix III

## Management's Response to the Draft Report

**Memorandum**

CITY OF DALLAS

DATE September 26, 2007

TO: Craig Kinton
City Auditor

SUBJECT: AT&T Managed Service Audit Response

Attached please find our response to your AT&T Managed Service audit issues.

Should you require additional information, please let me know.

Worris Levine, Jr.
Director/CIO
Communications & Information Services

c: Mary Suhm, City Manager
Jill Jordan, P.E. Assistant City Manager
Paul Garner, Assistant City Auditor
Charles Burki, Assistant Director, CIS
William Finch, Assistant Director, CIS

RECEIVED
SEP 2 7 2007
CITY AUDITOR'S OFFICE

"Dallas, Together We Do It Better"

## Management's Response Summary

**Recommendation 1:**

- The CIS Department and AT&T have implemented the policies and procedures necessary to fulfill all security contractual deliverables. The implementation of these policies and procedures removes any concerns of security failures.

- AT&T has agreed to credit the City of Dallas **$24,987.00**. This credit is based on the 9 months the contact was not compliant and AT&T added an additional 5 months of credits.

**Recommendation 2:**

- CIS has implemented organizational changes to ensure that the AT&T contract is properly monitored and in contract compliance. The Director/CIO of CIS has reorganized the organization and implemented a Contract Compliance / Contract Administration team to the AT&T contract.

---

### Audit Results:

### Management's Response

**Recommendation 1:**

- The CIS Department and AT&T have implemented the policies and procedures necessary to fulfill all security contractual deliverables. The implementation of these policies and procedures takes care of the contractual network security violations and vulnerability identified by the Auditor. Network security policies and procedures have been implemented in the areas of:
    - Intrusion Detection System (IDS) Signature updates (implemented April 22, 2007).
    - Critical Event Notification (implemented May 2007)
    - IDS License renewal (installed April 26, 2007)
    - Procedures for Back Ups of Firewall Configuration Firewall changes (implemented April 27, 2007)

  AT&T has implemented data capturing procedures to provide CIS with sufficient data to monitor results. These data capturing procedures provide reports to CIS in the areas of:
    - Bandwidth Utilization
    - Network Management and Service Level Agreement
    - Equipment and Telephony Services
    - Record Retention.
- AT&T has agreed to credit the City of Dallas **$24,987.00**. This credit is based on the 9 months the contract is not compliant.

**Recommendation 2:**

- CIS has implemented organizational changes to ensure that the AT&T contract is properly monitored and in contract compliance. The Director/CIO of CIS has reorganized CIS and implemented a Contract Compliance / Contract Administration team to the AT&T contract: The Contract Compliance / Contract administration team will:
  - Maintain documentation of the tests performed;
  - Evaluate the test results; and,
  - Compare test results against contract requirements