

Communications and Technology Services Performance Audit

Prepared for: Department of Information Resources

As of July 19, 2012

© 2012 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A. NDPPS 115222

Table of Contents

BACKGROUND	1
OBJECTIVES, SCOPE, AND METHODOLOGY	2
Objectives	2
Scope.....	2
Methodology	3
RESULTS	4
Overview of DIR’s CTS Division Billing System.....	4
Overview of CTS’s Staff Augmentation.....	5
Overview of CTS’s Organizational Structure.....	6
Overview of DIR’s Contract Fee Structure.....	7
Overview of DIR’s Network Security	8
Overview of DIR’s Disaster Recovery	9
FINDINGS AND RECOMMENDATIONS	10



KPMG LLP
Suite 3100
717 North Harwood Street
Dallas, TX 75201-6585

July 19, 2012

Andrew Dimas
Department of Information Resources
300 West 15th Street
Suite 1300
Austin, TX 78711

Dear Mr. Dimas:

This report presents the results of our work conducted to address the performance audit objectives relative to the Department of Information Resources' (DIR's) Statement of Work for the Communications and Technology Services (CTS) Division. Our fieldwork was conducted from May 24, 2012 through July 19, 2012.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The performance audit included an examination of four areas discussed in the Sunset Commission Report and was made in accordance with:

- Generally Accepted Government Auditing Standards (GAGAS); and
- The laws of the State of Texas (State).

The four areas are:

- Billing process and system;
- Cost-recovery fee and price-setting practices;
- Use of contractors in the telecommunications division and DIR's financial and oversight controls of staff augmentation contractors; and
- Overall administration and management, including organizational structure.

The audit objectives of our work were to determine the following:

- The billing process is efficient and effective and whether internal controls are in place to ensure the accuracy of the data;
- The billing system uses proper controls, is secured, and functions as intended;
- Management controls are in place to monitor the effective use of staffing augmentation;
- CTS's organizational structure is efficient and effective for CTS to perform and achieve its mission, goals, and objectives;
- The Texas Agency Network (Tex-AN) NG contracts ensure that service and fee structures are beneficial and cost-effective to the customers of CTS;



Andrew Dimas
Department of Information Resources
July 19, 2012

- CTS management provides adequate oversight of both internal and external resources to assure that the security of the networks is adequately monitored, that appropriate security policies are in place along with a mechanism to keep the policies and their enforcement up to date; and
- Disaster recovery policies and procedures exist, are followed, and how often they are administered.

As our performance report further describes, KPMG LLP (KPMG) identified the following findings as a result of the work performed to meet the above-stated performance audit objectives:

Disaster Recovery

- Although DIR has a disaster recovery plan in place, it has not been tested by DIR or the data center servicer. A disaster recovery plan for DIR was created by IBM, the data center servicer for State of Texas agencies through June 30, 2012. The disaster recovery plan was never tested by DIR or IBM. Xerox replaced IBM as the data center servicer on July 1, 2012. Xerox has a disaster recovery plan and will issue a schedule of testing by October 2012.

Billing System Security Controls

- The vendor supporting the NetPlus billing system has unrestricted access to the NetPlus application service account, and DIR does not actively monitor the vendor's use of the account.
- One NetPlus application service account and one NetPlus database service account (oracle) are granted administrative access to the operating system's root account; however, this privileged level of access is not required for the operation of the NetPlus application or database.
- Two NetPlus application accounts that are not assigned to a specific CTS employee were granted administrative rights and were only used during implementation; however, these accounts are not required for the operation of the NetPlus application.
- An inactive account existed on the NetPlus application/database server. This account did not have administrative rights and was locked upon notification by KPMG.
- DIR does not perform a periodic review of Netplus application or operating system accounts.

Billing Process

- In performing procedures over the billing process, we determined the dispute tracking and resolution process for errors in vendor invoices is manually performed and is not designed to be scalable to meet future needs.

Based upon the performance audit procedures performed and the results obtained, we have met our performance audit objectives. Included in the attached report, are our detailed findings and recommendations for the aforementioned audit objectives.



Andrew Dimas
Department of Information Resources
July 19, 2012

This performance audit did not constitute an audit of financial statements in accordance with Government Auditing Standards. KPMG was not engaged to, and did not, render an opinion on the DIR's internal controls over financial reporting or over financial management systems (for purposes of OMB's Circular No. A-127, Financial Management Systems, July 23, 1993, as revised). KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

Very truly yours,

KPMG LLP

Background

Government Code Chapter 2170 authorizes the Department of Information Resources to provide telecommunication services to state agencies. These services are provided by DIR's CTS Division. CTS delivers these services through the Tex-AN. CTS manages the Tex-AN statewide communications system through negotiated contracts with providers for a number of network communications solutions at a cost savings to state agencies and other eligible public sector entities.

In fiscal year 2012, following a competitive procurement, CTS awarded service contracts to multiple vendors to provide customers with several options to choose for telecommunication services. This multi-vendor sourcing approach is designed to provide agencies with greater choice in the services offered and via vendor competition drive costs down. This multivendor sourcing approach is considered a leading practice for purchasing telecommunication services.

In addition to negotiating and establishing contracts with vendors, DIR is also responsible for establishing cost recovery fees as well as billing customers for usage of CTS service.

The Texas Sunset Advisory Commission recommended an audit of CTS covering the following areas:

- Billing process and system;
- Cost-recovery fee and price-setting practices;
- Use of contractors in the telecommunications division and DIR's financial and oversight controls of staff augmentation contractors; and
- Overall administration and management, including organizational structure.

Objectives, Scope, and Methodology

Objectives

The performance audit objectives of our work related to the Auditee were to:

Billing Process and System

- Determine whether the billing process is efficient and effective and whether internal controls are in place to ensure the accuracy of the data.
- Determine whether the billing system uses proper controls, is secured, and functions as intended.

Cost-recovery fee and price-setting practices

- Determine whether the Tex-an NG contracts ensure that service and fee structures are beneficial and cost-effective to the customers of CTS.

Use of contractors in the telecommunications division and DIR's financial and oversight controls of staff augmentation contractors

- Determine whether management controls are in place to monitor the effective use of staffing augmentation.
- Determine whether CTS management provides adequate oversight of both internal and external resources to ensure that the security of the networks is adequately monitored, and that appropriate security policies are in place along with a mechanism to keep the policies and their enforcement up to date.
- Determine whether disaster recovery policies and procedures exist, are followed, and how often they are administered.

Overall administration and management, including organizational structure

- Determine whether CTS's organizational structure is efficient and effective for CTS to perform and achieve its mission, goals, and objectives.

Scope

The scope of this performance audit was to review DIR's CTS Division to fulfill the Texas Sunset Advisory Commission (Sunset) report recommendation calling for a comprehensive audit of CTS. We did not perform a comprehensive audit of the DIR's overall accounting system. In performing our procedures, we considered internal controls related to our performance audit objectives, but we did not perform an audit of internal controls.

We conducted our performance audit in accordance with *Government Auditing Standards*. Those standards require that we plan and perform the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our performance audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our performance audit objectives.

DIR is responsible for establishing and maintaining an acceptable CTS billing system. DIR is also responsible for establishing and maintaining adequate processes and internal controls to do so in accordance with government accounting and reporting requirements. Our responsibility is to provide findings and conclusions based on the results of the performance audit.

Methodology

As part of the performance audit of DIR's CTS Division, we:

- Obtained an understanding of the billing system's functionality
- Evaluated the internal controls for billing data accuracy
- Evaluated the billing process for efficiency and effectiveness
- Evaluated the internal controls for billing system security
- Obtained an understanding of management control processes used for staff augmentation
- Evaluated the effective use of staff augmentation
- Obtained an understanding of the current CTS organizational structure
- Obtained an understanding of the CTS mission, goals, and objectives
- Evaluated the CTS organizational structure in comparison to similar organizations
- Obtained an understanding of the process used by CTS to forecast revenue and the cost of funding the CTS organization
- Obtained an understanding of the mark-ups applied to services purchased via the Tex-AN NG contract
- Evaluated the fee mark-up structure in comparison to other similar organizations
- Obtained an understanding of DIR's network monitoring and security responsibilities
- Obtained management oversight processes and procedures of internal and external resources
- Evaluated the adequacy of network monitoring that is performed
- Obtained network security policies
- Evaluated how policies and their enforcement up to date
- Evaluated network alert notification process and procedures
- Obtained an understanding of DIR's disaster recovery obligations
- Obtained disaster recovery policies and procedures
- Evaluated how often disaster recovery procedures are administered.

Results

Overview of DIR's CTS Division Billing System

DIR provides technology services to state agencies and other eligible entities. DIR obtains discounted pricing through volume purchasing, and does not engage in contracts where a minimum usage is required. For telecommunication services specifically, DIR manages the Tex-AN New Generation (NG) contracts. A service catalog listing pricing for telecommunication vendors and products assists customers in ordering products and services from DIR.

CTS utilizes NetPlus, a vendor-supported application, to process telecom orders and billing. The NetPlus server is located at the Data Center in Austin and runs on a Solaris server and an Oracle database. The server is hosted by Xerox, which replaced IBM on July 1, 2012. Both Xerox and DIR employees have administrative and unprivileged accounts on the server and database, and each organization is responsible for its accounts on the server.

Ordering

The Order Department enters telecom orders into the Remedy system (Ordering Remedy), which interfaces with NetPlus. If inaccuracies are noted during a manual review of the new NetPlus record, the Billing Coordinator notifies the Orders Group to take corrective action. Service start and end dates, non-recurring charges (NRCs), and prorated amounts are manually entered into NetPlus by the Order Department.

Billing and Accounts Receivable

A consolidated bill is sent to each CTS customer for their inventory of telecom services, using the usage, rate information, and charges in NetPlus. For telephone usage, vendors supply a daily usage report by phone number, which is uploaded daily into NetPlus. Other monthly recurring charges (MRC) are billed as per the service record configured in NetPlus.

Billing periods are programmed into NetPlus, and vendor services can vary and are stored in each vendor's Billing Management Plan. Billing charges include the following:

- Usage (telephone minutes only, reported by vendors daily and uploaded into NetPlus)
- MRC (billed monthly based on service rates in NetPlus)
- NRC, e.g., for installation fees or other one-time charges
- Additional fees and surcharges, if not included in the recurring charges
- A cost recovery fee (CRF), currently 12 percent for most services. Services that are not subject to the 12 percent CRF include fees charged by a tax district or E-rate participants who receive refunds from the federal government for certain telecommunications costs. These exceptions are reviewed on a case-by-case basis. The CRF funds the operation of the CTS program and is established during the annual budget process with approval by the DIR board of directors. DIR's statutory authority to collect the CRF is established by Texas Government Code 2170.057.

Billing Disputes – CTS Customer

CTS customers are responsible for reviewing the accuracy of their monthly bill. Disputes raised by CTS customers are entered into the Billing Department's Remedy System (Billing Remedy) and are investigated by CTS personnel. The CTS customer generally does not pay the disputed amount until the dispute is cleared.

Vendor Invoices and Accounts Payable

Vendors operating under the Tex-AN NG contracts produce invoices that contain required data as outlined in the DIR Vendor Reporting Guide. Each vendor's Tex-AN NG Monthly Consolidated Invoice (which includes the Detailed Monthly Invoice File) is uploaded to DIR's FTP site each month. A few vendors with legacy contracts, which do not operate under Tex-AN NG, provide invoices based on previous agreements. Invoices received from these vendors must be manually entered into the NetPlus.

The Detailed Monthly Invoice File is exported to an Excel spreadsheet and imported into a Microsoft Access database, known as the Cost Management database. The database has a billing table for each vendor for usage charges, MRCs, NRCs, and adjustments. A file of charges billed to customers is interfaced from NetPlus into the Cost Management database. Vendor invoices for NRCs, prorated charges, and adjustments are not validated in the database, but are checked manually against the information from NetPlus. DIR utilizes various queries against the cost management database to validate invoice data and to identify differences between vendor invoicing and CTS customer billing. Any differences identified are investigated by CTS personnel.

Vendor Disputes

The differences (disputes) identified on the exception queries are investigated and tracked in a spreadsheet. Once the dispute is resolved, a new vendor invoice is sent with an adjustment in the adjustment section. The billing administrator manually updates corrections in NetPlus if required. Any debits or credits resulting to a customer's bill are reflected in the next billing period.

Overview of CTS's Staff Augmentation

CTS is responsible for managing the statewide communications infrastructure that provides voice, video, and data, including integrated voice response, telephony, wide area network, virtual private network, and call center solutions to more than 700 state and local government agencies including directly supporting the Capital Complex Telephone System (CCTS).

Use of Staff Augmentation

Historically, CTS has utilized staff augmentation resources to supplement CTS staff in support of their mission and objectives. Based on various project needs, CTS engages staff augmentation resources to support agency-approved projects. The actual cost of staff augmentation resources is billed to the respective agency utilizing the resource. As of the date of this report, no staff augmentation resources are being utilized by CTS.

Staff Augmentation Controls

CTS has formally documented policies and procedures related to staff augmentation, based on documentation obtained and discussions with CTS personnel, procedures appear to be in place to govern the use of staff augmentation.

Overview of CTS's Organizational Structure

DIR provides technology services to state agencies and other eligible entities (e.g., Texas municipal governments, educational entities). CTS manages the statewide communications infrastructure that provides voice, video, and data, including integrated voice response, telephony, wide area network, virtual private network, and call center solutions to more than 700 state and local government agencies. These services are provided via a multivendor sourcing approach.

In fiscal year 2012, DIR had a total of 748 customers that utilized CTS service: 367 municipal governments, 139 state agencies, 239 educational entities, and 3 categorized as other.

The services managed by CTS include:

- Local Services including: business line, PBX trunk, Primary Rate Interface (PRI), Basic Rate Interface (BRI), and Operator services
- Voice Over Internet Protocol (VOIP) including: Managed PBX, and IP telephone
- Long Distance Services including: inbound calling, outbound calling, circuit switch digital
- Data Services including: Multiprotocol Label Switching (MPLS), and point-to-point data circuits
- Internet
- Metro Ethernet
- Small Office/Home Office (SOHO)
- Wireless broadband
- Fixed satellite services
- Capital Complex Telephone System (CCTS).

The vendors providing these services include: AT&T, Twtelecom, Level 3, Century Link, Windstream, Time Warner Cable, Verizon Business, Hughes, Skyfiber, and Proactive.

CTS Mission, Goals, and Objectives

The mission of DIR is to provide technology leadership, solutions, and value to Texas state government, education, and local government entities to enable and facilitate the fulfillment of their core missions. Specifically, "The services DIR provides to Texas state government, education, and local government entities will focus on excellence through quality of service, responsiveness, innovation, professionalism, and teamwork and we will operate in an open, ethical, efficient, and accountable manner, with high regard for all customers."

The key objectives for CTS in fiscal year 2012 include:

- Deliver thought leadership for the State and all DIR customers
- Create and implement solutions that reduce costs and maximize productivity
- Provide value-added services at the highest level of quality.

Comparing CTS Organization Structure

Texas's relative decentralized form of government drives the need for CTS to have a broader mission and set of objectives than comparable organizations that have a more centralized form of government. Most states have a centralized authority, which is responsible setting and overseeing telecommunication standards from an enterprise level. In several instances, these more centrally managed states also have consolidated the budget and purchasing authority away from the State agencies. Regarding the CTS mission and objectives, they appear to be consistent with other comparable organizations. It should be noted however that given the size and complexity of the State organization, a limited number of states are available that can be used for comparative analysis.

Overview of DIR's Contract Fee Structure

Government Code Section 2170.057 establishes DIR's statutory authority to collect amounts needed to operate the CTS program.

DIR has established and documented a formal process for evaluating, setting, and communicating the administrative fee for CTS. DIR undergoes a formalized process for fee setting establishment on an annual basis. DIR then monitors financial operating throughout the year to determine if enough revenue is being generated to recover costs.

DIR's fee setting methodology for CTS is based on the following characteristics:

- Forecast of customer consumption;
- Determine operating expenses to be recovered by administrative fees; and
- Set fees at levels that will recover operating costs, inclusive of unexpended balance authority and forecasted customer consumption.

CTS's primary focus is to serve state agencies; however, there are significant numbers of voluntary customers, such as higher education institutions, public school districts, and local governments, that can purchase services directly. The 748 CTS customers are comprised of local government (367 entities), state agencies (139 entities), educational entities (239 entities), and 3 are categorized as other.

Forecasting consumption for these customers adds complexity to the forecasting model because consumption maybe impacted by factors external to the state appropriations process. Further complicating the forecasting model is the flexibility of service offerings, which provides incentives for customers to migrate to newer technologies, which result in lower CTS revenue. This forecasting challenge is a consistent challenge faced by other states with similar telecommunication contracts.

Comparing CTS's Fee Structure

DIR has established the following mark-ups on service to recoup the cost associated with the CTS organization:

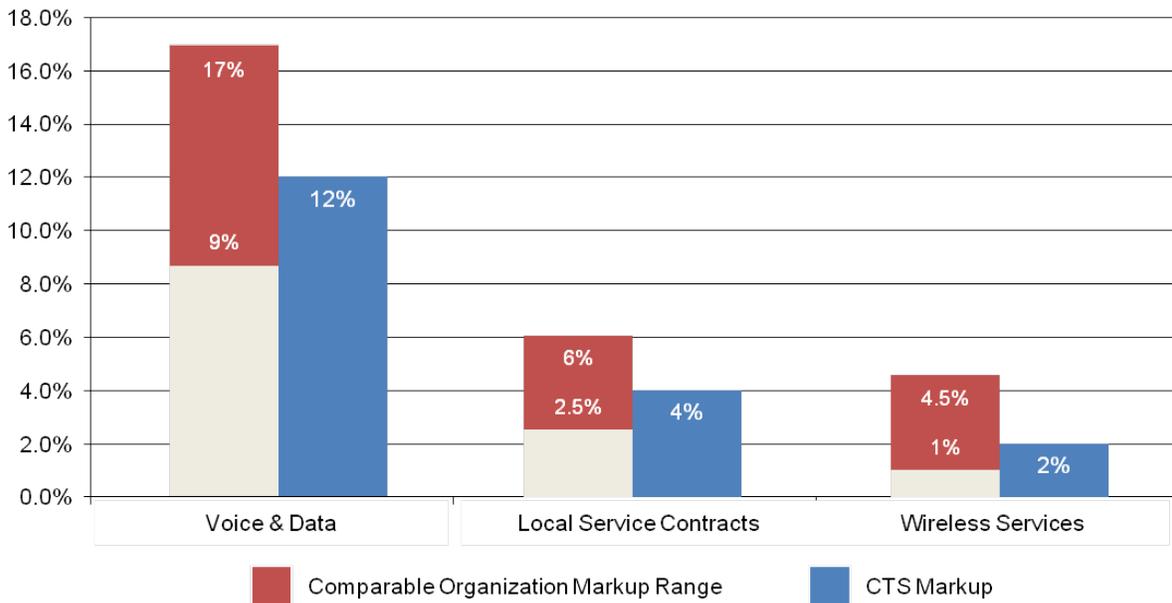
- Forecast of customer consumption;
- Determine operating expenses to be recovered by administrative fees;
- Expenses include DIR owned capital equipment and the maintenance of DIR owned capital equipment used to support TEX-AN and the Capitol Complex Telephone System (CSTS); and
- Set fees at levels that will recover operating costs, inclusive of unexpended balance authority and forecasted customer consumption mark-up

Establishing a reasonable set of comparables to the Tex-AN NG contract is challenging given the size, scope of services, contract participants, and enabling services offered by DIR. Our analysis indicates that the Tex-AN NG fee structure is market competitive and other states are considering moving toward multivendor telecommunication solutions. In summary, we determined the following:

CTS’s overhead for telecom administrative and billing support of approximately 3.1 percent of the mark up is at the low end of the market comparable range of 3 percent to 5 percent. This market comparable included other large states, federal agencies, and large commercial clients.

CTS contract fee structure is aligned with comparable organizations (large states and federal agencies):

- Voice service contract mark-up range is 9 percent to 17 percent – CTS mark-up is in range at 12 percent
- For local services contract mark-up range is 2.5 percent to 6 percent – CTS mark-up is in range at 4 percent
- For wireless services contract mark-up range is 1 percent to 4.5 percent – CTS mark-up is in range at 2 percent



Overview of DIR’s Network Security

Per HB 3112 Section 2059.056, if the department provides network security services for a state agency or other entity, the department is responsible for network security from external threats for that agency or entity. To that end, DIR operates a Network Security Operations Center (NSOC) in conjunction with AT&T to provide security monitoring for networks communicating with the Internet. A statement of work between DIR and AT&T is in place and governs the creation of the NSOC and the service level agreements (SLAs) of each party for its operation. DIR management and AT&T review compliance with the SLAs at weekly meetings. Status of each SLA is tracked in a spreadsheet as well as the dispositions of variances that are noted.

DIR responsibilities include, but are not limited to, providing sufficient personnel to facilitate AT&T's support and tools, maintaining equipment, furnishing contact and escalation lists, and background checks. While DIR has responsibility to manage security for external threats, any threats detected on the internal networks are the responsibility of the State agency on whose network the threat resides. DIR will notify the State agency information security officer, but does not take action to enforce remediation unless requested to do so by the agency.

AT&T responsibilities include, but are not limited to, continuous management and monitoring of gateway IPS devices, and security management, monitoring, and maintenance of IDS devices. In addition, AT&T maintains vendor maintenance contracts pertaining to the IPS and associated equipment and providing continuous security alerts and analysis of threat information. AT&T provides monthly performance and SLA reports, and provides controlled penetration tests and vulnerability assessments on request, and assistance to remedy resulting issues. AT&T uses the netForensics and Security Event Threat Analysis (SETA) platforms to monitor network traffic and immediately notifies DIR if signatures of suspicious activity occur. Action is taken such as blocking the IP address ranges of the source of malicious activity. A weekly meeting is held by DIR management to evaluate the top threats and level of compliance with contract terms by both DIR and AT&T. Any issues noted and actions taken for remediation (or the status of such actions) are recorded in a spreadsheet against each applicable requirement.

Overview of DIR's Disaster Recovery

Under the IBM Team for Texas contract, a comprehensive disaster recovery (DR) plan was issued by IBM Global Services, which was in effect until June 30, 2012. Effective July 1, 2012, Xerox replaced IBM as the data center servicer.

The IBM DR plan provides a plan for recovery of DIR services through restoration from backup media and, if required, installation of recovery equipment and media at the Austin Disaster Recovery Operations Center (ADROC). The Disaster Recovery Coordinator, noted as John O'Sullivan, has overall responsibility for the plan activities. DIR has reviewed their active IT applications and rated the importance of the data in each area. The NetPlus application and database server is rated as critical to DIR and its customers, with a recovery time objective of two days.

The DR plan calls for management review of the plan and updates to be made to the plan at least once a year; however, the most recent version of the IBM plan is dated May 14, 2009. In addition, DR testing has not been performed by IBM, and DIR did not perform server DR testing outside the scope of the IBM plan.

Under the Xerox contract beginning July 1, 2012, a new DR plan will be issued and in October 2012, a testing schedule is to be released that will list agency DR testing by criticality of the agency services. Currently, ACS offers classes on DR and business continuity to eligible participants as part of their services.

Findings and Recommendations

<p>DISASTER RECOVERY –</p> <p>Condition:</p>	<p>Although DIR has a disaster recovery plan in place, it has not been tested by DIR or the data center servicer. A disaster recovery plan for DIR was created by IBM, the data center servicer for State of Texas agencies through June 30, 2012. The disaster recovery plan was never tested by DIR or IBM. Xerox replaced IBM as the data center servicer on July 1, 2012. Xerox has a disaster recovery plan and will issue a schedule of testing by October 2012.</p>
<p>Criteria:</p>	<p>TAC 202.24 requires written Business Continuity Plans that address information resources so that the effects of a disaster will be minimized, and the state agency will be able either to maintain or quickly resume mission-critical functions.</p>
<p>Effect:</p>	<p>A disaster recovery plan that is not tested periodically increases the risk of critical systems not being restored in a timely manner to resume operations in case of a disaster.</p>
<p>Cause:</p>	<p>IBM did not perform tests of the existing disaster recovery plan covering the CTS servers.</p>
<p>Recommendation:</p>	<p>Management should review the Xerox disaster recovery plan for completeness, and ensure a testing schedule is established and testing of the plan be performed on an annual basis.</p>
<p>Auditee Response:</p>	<p>We concur with this finding and will work with Xerox and Cap Gemini to revise as needed the disaster recovery plan. Further, the plan will be tested in FY13 according to the datacenter plan to be published in October. The agency does monitor the daily and weekly status of system backups and ensures that all backups are completed successfully.</p>

<p>BILLING SYSTEM SECURITY CONTORLS –</p> <p>Condition:</p>	<p>CTS utilizes NetPlus, a vendor-supported application, to process telecom orders and billing. Access to telecommunication data can be accessed through the NetPlus application, through the Oracle database, or through the Solaris server hosting the NetPlus application and the Oracle database. Access to the NetPlus application and Solaris server was not restricted appropriately, and KPMG noted the following:</p> <ul style="list-style-type: none"> • The vendor supporting NetPlus has been granted administrative access to the Solaris server through an application service account, through which the vendor can access the server and make program changes to the application. DIR does not have a process to help ensure the vendor is only accessing this account during approved sessions. • One application and one database service account on the Solaris server are granted administrative privileges, which is not required for operation. • No periodic review is performed by DIR or IBM of their respective users and their privileges on the Solaris server or Oracle database. A review of Active Directory users is performed; however, access to the database and server is not subject to Active Directory authentication. • Two of 12 NetPlus application accounts with administrative access have been inactive since the initial configuration of the application.
<p>Criteria:</p>	<p>Logical access to the NetPlus application, Solaris server, and Oracle database should be restricted to appropriate personnel, and system controls should be in place to help ensure the accuracy and timeliness of telecommunication billings.</p>
<p>Effect:</p>	<p>Logical access weaknesses increase the risk of unauthorized access to NetPlus application, the operating system, and database. In addition, unauthorized access could result in inappropriate changes made to CTS customer or vendor data, or unintentional changes made to the program by the vendor.</p>
<p>Cause:</p>	<p>Based on inquiry with management, KPMG noted the following:</p> <ul style="list-style-type: none"> • The vendor developers are granted access to the Solaris server in order to provide development assistance based on a customization request or emergency fix required by DIR. • The application service account is granted administrative access to allow the application vendor to more easily apply changes to the production environment. The database service account is an inactive account. • While a review was performed of Active Directory users, which controlled access to the application, the assumption was made that this also covered access to the Solaris server or Oracle database when in fact users not on the DIR domain can access the database and server. According to the division of responsibilities between IBM and DIR, IBM should review their users on the server and database, and DIR should review their users. In fact neither entity reviewed users at the server or database level. • The accounts existed for setup and configuration purposes, but have not been removed or disabled.

<p>Recommendation:</p>	<p>DIR should consider implementing the following:</p> <ul style="list-style-type: none"> • Developer access to the application should be disabled when not required for vendor support purposes. When vendor access is required, the access should be monitored and disabled when not required for vendor support. • The application and database IDs should not be granted administrative access to the server, as privileged access is not required to run the software. • DIR should be aware of and periodically review users for whom responsibilities are managed by DIR on the database and server, as unmonitored user IDs could result in a risk to the integrity of the billing data and the program code through inappropriate access. In addition, DIR should monitor the completion of the periodic review of Xerox’s users by Xerox. • DIR should immediately disable IDs deemed no longer to have a purpose on the application, database, or server.
<p>Auditee Response:</p>	<p>The agency concurs with the findings. The vendor Ventraq does have access to the production and test systems because the system is a Commercially-Off-The-Shelf system (“COTS”) that requires periodic operational support from the vendor. However the overall access has been reviewed and changed to eliminate root access and implementation accounts have been removed from the system. Ticket REQ-2925 was submitted to Xerox to remove Oracle from the appropriate file. A review of the Solaris OS and Oracle database accounts on the applicable server was performed by the Information Security Officer on July 12, 2012, and the findings were recorded in SalesForce. This review will take place quarterly going forward.</p>

<p>BILLING PROCESS –</p> <p>Condition:</p>	<p>In performing procedures over the billing process, we determined the dispute tracking and resolution process for errors in vendor invoices is manually performed and is not designed to be scalable to meet future needs. The AP and AR processes are only partially automated as some subprocesses are manually intensive.</p>
<p>Criteria:</p>	<p>Controls are in place to help ensure the billing of telecommunications services is efficient and effective.</p>
<p>Effect:</p>	<p>Disputes that are not resolved timely could impact the efficiency and effectiveness of the telecommunication billing process. The manually intensive processes increase the risk of errors and can cause delays in determining the resolution of the disputed amount. In particular, the dispute resolution process for vendor invoices requires a significant amount of investigation and manual resolution, and usually requires at least a month to resolve. The adjustments made to CTS customer accounts as a result of the dispute could take months to determine.</p>
<p>Cause:</p>	<p>Disputes are investigated manually based on exception reports produced from the Cost Management database. These reports are based on automated inputs from the NetPlus application and vendor invoices, in addition to manual inputs for specific services and issues.</p>
<p>Recommendation:</p>	<p>DIR should consider implementing a more automated process to resolve vendor invoice disputes if anticipated growth in CTS customers is expected.</p>
<p>Auditee Response:</p>	<p>With regard to the audit finding concerning the billing system dispute tracking and resolution processes, we concur with the audit recommendation that DIR should consider implementing a more automated process. The DIR Billing department is exploring options to convert the current dispute tracking file to an uploadable format. The Billing department will then upload disputes to a tracking system for better automation of the dispute resolution process. Estimated completion date is January 31, 2012.</p>