TEXAS DEPARTMENT OF INFORMATION RESOURCES

P.O. Box 13564 ◆ Austin, TX 78711-3564 ◆ www.dir.state.tx.us
Tel: (512) 475-4700 ◆ Fax: (512) 475-4759

November 4, 2008

VIA ELECTRONIC AND CERTIFIED MAIL

Ken Weiss
Vice President, State of Texas Data Center Services
International Business Machines Corporation
400 W. 15th Street, Suite 1200
Austin, Texas 78701

Mark S. Hicks, Esq.
International Business Machines Corporation
9229 Delegate's Row
Precedent Office Park, Building 81
Indianapolis, Indiana 46240-3810

General Counsel, Americas—Global Technology Services
International Business Machines Corporation
294 Route 100
Somers, New York 10589-0100

RE: Notice to Cure Breaches of the Master Services Agreement (dated November 22, 2006) between the State of Texas, acting by and through the Texas Department of Information Resources, and International Business Machines Corporation

Gentlemen:

I write to inform you that under section 20 of the Master Services Agreement ("MSA"), International Business Machines Corporation ("IBM") has breached its contractual duties and obligations to the State of Texas. Specifically, I hereby notify you that the numerous breached MSA provisions include, but are not limited to, Section 13.2 (b) Safeguarding DIR Data, Exhibit 2.3 Section 2.6.1.12 Operations and Processing, Section 2.11 Backup and Recovery Services, and Section 3.1.10 Operations. By this Notice to Cure, IBM is hereby notified that it has thirty (30) days to remedy the numerous breaches described in this letter.

As you know, the MSA requires IBM to protect and preserve state data by ensuring that information stored on IBM servers is adequately backed-up. Despite those requirements, IBM has repeatedly failed to adequately implement contractually mandated data-backup mechanisms. On multiple occasions, the Texas Department of Information Resources ("DIR") has instructed IBM to remedy its inadequate performance. However, IBM has consistently failed to do so and has therefore failed to satisfy its Service Level Agreement ("SLA") with the State.

Specifically, in October, 2007, DIR instructed IBM to inventory all affected state agencies' backup environments to ensure all required systems were being adequately protected. Although the inventory we requested was ultimately completed, it revealed that the backup processes were inadequate because they did not accurately preserve the State's data.

In March 2008, DIR formally notified IBM that its performance of the contract was inadequate and that improved performance was necessary to satisfy the MSA. That correspondence specifically informed IBM that it needed to improve the accuracy of its data backups. In August 2008, DIR requested that IBM prepare and execute a backup remediation plan. As of this writing, that plan has not been successfully implemented and IBM still has not yet demonstrated that it can comply with the MSA's data backup requirements. The current, unremediated situation is untenable for the State of Texas, as critical state data continues to be at risk.

The following acts or omissions by IBM constitute breaches under the MSA:

1. IBM has repeatedly failed to meet DIR's request to provide data backup remediation.

2. IBM failed to adequately implement data backups, which resulted in data losses.

3. IBM failed to provide evidence that data-backup failures were corrected.

4. IBM failed to consistently provide required backup-failure documentation in the Remedy System, which led to inaccurate SLA achievement metrics.

5. IBM failed to develop a process that ensured all the appropriate backups were scheduled and executed.

6. IBM failed to consistently maintain data-backup logs, which indicate data-backup jobs' success or failure.

7. IBM failed to implement processes that periodically test and verify whether data can be restored in manner that is usable after restoration.

8. IBM failed to consistently backup data and systems at remote sites, and failed to store remote site backup tapes off-site.

In order to comply with the MSA's backup and recovery requirements:

1. IBM must complete and review a data backup gap analysis for each affected state agency. For each server, mainframe and storage device under IBM's control, IBM must identify the data files that require backups and the status of the backup. Before this requirement is considered satisfied, the affected state agency must independently validate IBM's remedial efforts. Finally, IBM must provide evidence that a backup schedule has been implemented and that an actual data backup has been successfully performed.

2. IBM must document and implement policies and procedures that report when it has completed scheduled backups.

3. IBM must document and implement policies and procedures that successfully remedy an unsuccessful backup within 24 hours.

4. IBM must create a Remedy System incident ticket for each unsuccessful backup so that SLA metrics accurately reflect IBM's performance of the MSA.

5. IBM must provide each agency with a weekly report that identifies all scheduled and unscheduled backups. These reports must document whether each backup was successful or unsuccessful, full or incremental and the age of the newest restorable backup.

6. IBM must document and execute policies, procedures and reports that demonstrate its ability to archive backup logs for 13 consecutive months. That documentation must be usable for validation and auditing purposes.

7. IBM must document and execute policies, procedures and reports that demonstrate an enterprise approach to the periodic testing of backup files. This backup file testing must confirm that data can be restored in a form that is complete and functional.

8. IBM must document and execute policies, procedures, and reports that demonstrate a standardized off-site tape management procedure for every backup tape created.

Given the significance of the MSA breaches by IBM and the impact those breaches have on the integrity of state data, IBM must respond to this Notice to Cure within ten (10) days, not later than noon, Central Standard Time, November 14, 2008. That response must contain a detailed plan to cure IBM's MSA breaches, including the date by which IBM will satisfy the requirements stated above and therefore the MSA.

To protect the integrity of state data, IBM must move swiftly to implement the above referenced remediation plan. Until we are assured that affected information resources are being backed-up and that IBM is satisfying the MSA's data security requirements, the State cannot resume data center consolidation under the MSA.

Sincerely,

Brian S. Rawson

Brian S. Rawson
Executive Director
Chief Technology Officer-State of Texas Dept. of Information Resources