JLARC
JOINT LEGISLATIVE AUDIT AND REVIEW COMMISSION

JLARC Summary
Agilysys Audit of the State Data Center Computer Outage

On August 25, 2010, the Commonwealth's data center in Chester (CESC) experienced a major outage that affected more than 26 State agencies. An audit of the outage and Northrop Grumman's response to restore services was conducted by Agilysys, a provider of information technology services to Fortune 50, 500 and mid-tier customers. Agilysys was selected following a competitive process that involved the Governor's Chief of Staff, the Secretary of Technology, the Commonwealth's Chief Information Officer, Virginia Information Technologies Agency staff, the Director of the Joint Legislative Audit and Review Commission (JLARC), and JLARC staff.

Following completion of the audit, Northrop Grumman (NG) was given two opportunities to review the audit and submit factual corrections along with supporting documentation. NG was also allowed to submit a formal written response to include in the audit. As part of a long established process when working with consultants, JLARC staff worked with Agilysys to ensure the audit was factually correct and the findings were presented in a manner that could be understood by the general reader.

The following are the primary findings from the Agilysys audit:

- The outage resulted from the failure of a key data storage system (DMX-3) and subsequent human error during its repair, but the primary cause of the failure remains unknown.
- Loss of data, and the delay in restoring operations and data, resulted from NG's failure to follow two key industry best practices.
- NG is not fully using industry best practices for monitoring, testing, and management, which hindered NG's response to the outage.
- In Agilysys's professional opinion, the deficiencies "represent an insufficient degree of self-governance towards continuous process improvement and the management of risk in the environment."
- Many components selected for the data center and its IT infrastructure meet or exceed industry best practices, but implementation falls short.

Additional detail for each finding is presented on the reverse side.
For more information, contact us at 804-786-1258 or info@jlarc.virginia.gov.

The outage resulted from the failure of a key data storage system (DMX-3) at the CESC data center and subsequent human error during its repair, but the primary cause of the electrical fault leading to the failure is unknown.

- An unknown electrical fault caused component failures, but neither NG's Root Cause Analysis, nor any other information presented by NG, states why or when the fault occurred, or how to prevent a future fault.
- Although the DMX-3 is a best-of-breed system, redundant components produced errors simultaneously, indicating a need for corrective action.
- The outage itself was triggered by an erroneous decision by an NG subcontractor regarding which component to repair first.

Loss and corruption of data, and the delay in restoring operations and data, resulted from NG's failure to follow two key industry best practices.

- Failure to make point-in-time copies of data (known as "snapshots" or "clones") lengthened time to restore corrupted data.
- In the absence of snapshots, the failure to stop the real-time process used to copy (or "replicate") data from the CESC data center in Chester to the Southwest data center (SWESC), during the time when the DMX-3 was undergoing repair, led to corruption of data at SWESC.
- These failures also led to loss of data and corruption of the "catalog" used to track and index the location of agency data in the enterprise backup system.

Agilysys also found that NG is not fully using industry best practices to monitor, test, and manage IT operations, and may have insufficient staff, which hindered NG's response to the outage.

- Server monitoring is performed but without needed information on how server outages affect applications.
- Backup and network testing procedures are inadequate.
- Use of multi-step, decentralized backup process introduce delays and risk.
- NG may not have enough staff.

In Agilysys's professional opinion, the deficiencies "represent an insufficient degree of self-governance towards continuous process improvement and the management of risk in the environment."

- Contract requires NG to "use industry best practices" to avoid and mitigate "any material adverse effect" on continuity and quality of IT services (§ 3.1.2).
- Audit makes 20 unique recommendations for specific improvements.

Many components selected for the data center and its IT infrastructure meet or exceed industry best practices, but implementation falls short.

- The selection and design of several systems—server computer monitoring (HP OpenView), the DMX-3, redundancy of the core network, the fault tolerance and redundancy of the data center—meet or exceed best practices.
- As indicated earlier in this summary, NG's implementation of these and other aspects of the CESC data center often do not meet best practices.