SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN CUSTOMS SERVICE

Question No. 88

Senator Ludwig asked the following question at the hearing on 17 February 2006:

Outage of 24 January 2006 at the Burwood centre caused by the failure of a cooling fan:
a) what contractual obligations are there to test the system for redundancy arrangements.
b) on what dates was the system tested.
c) please provide a copy of the review of the maintenance arrangements at Burwood

The answer to the honourable senator's question is as follows:

a) The contractual obligations for the Burwood Centre relate to agreed levels of systems availability rather than for specific redundancy measures. The Burwood Centre as a purpose-built facility does have testing arrangements for maintenance activities including power cutover to battery and diesel generators. These tests are performed on a regular basis

b) The generators, UPS and other critical infrastructure are checked daily (during maintenance rounds), with a weekly maintenance check conducted on every Friday. A diesel load test is conducted every month.

c) See report below

CMR Infrastructure Audit – Feb 2006
Infrastructure Redundancy Assessment

Overview:

A physical audit of the CMR infrastructure environment at EDS' Burwood Operation Facility has been undertaken. The audit concentrated on redundancy availability and failover capability of all components of the CMR infrastructure and included power, network connectivity and alternate hardware.
The audit covered the following areas:
- External Client connectivity
- CCF Perimeter environment
- AIX and Wintel devices
- Storage environments
- Mainframe and Data Warehouse devices
- Network connectivity and inter-connectivity

Whilst the audit did verify the majority of the environment is implemented with correct redundancy through the power and network connections, there were a small number of areas identified where there is risk to the redundancy mechanisms.

CMR related infrastructure vulnerabilities:
(Note: In order to classify this document as Unclassified, items in parentheses ("") below have had their labels changed from actual device names.)

	Device	Vulnerability	Risk	Suggested Solution	Expected time-frame
1	External connection: Internet switches.	Powered from different circuits running from the same PDU.	Risk = low: Unlikely event but would result in loss of both Internet connections if main PDU is lost.	(If considered significant): Re-power second Internet carrier onto a 2nd PDU board Circuit	Change window only. Circuit already available.
2	External connection: "Client A" primary and Secondary NTU's	Plugged into same power circuit.	Risk = medium: loss of both primary and secondary paths for "ClientA" if circuit is tripped.	Re-Power "ClientA" Secondary from alternate circuit.	Change window only. Circuit already available.

3	External connection: "Client B" business NTU's	Powered from different circuits running from the same PDU.	Risk = low: Unlikely event but would result in loss of both primary and secondary paths for "ClientB" if main PDU is lost.	(If considered significant): Re-power Secondary onto a 2nd PDU board Circuit	Change window only. Circuit already available.
4	Perimeter: All perimeter equipment contained in C Class cabinets	Circuits daisy chained between the 4 C Class cabinets covering both primary and redundant equipment.	Risk = high: loss of primary and redundant paths through perimeter if one of 3 circuits trip.	Provide new circuits for BK11 (3), BL11 (3) and BM 11 (1). Ensure adequate PDU distribution.	Requires new power circuits to be run (may also require new PDU to be established in room) estimate 3-4 weeks.
5	DMZ (Unicentre): "SERVER001"	Dual power supplies but both in same circuit.	Risk = medium: loss of Unicentre DSM if power circuit is tripped.	Re-power 2nd PSU from alternate circuit (ACS 1/13).	Change window only. Circuit already available.
6	DMZ (Unicentre): "SERVER001"	Dual network links but both patched to same switch.	Risk = medium: loss of DMZ Unicentre DSM if switch fails.	Re-patch 2nd nic to alternate switch	Change window only. Alternate switch port already available.
7	ICZ (P590 switches): "SWITCH001"	Powered from same circuit. Only one circuit available to rack.	Risk = high: Loss of P590 ICZ network connectivity if circuit trips.	Provide new power circuit and re-power switch from new circuit.	Requires new power circuit to be run estimate 3-4 weeks.
8	ICZ (Unicentre): "SERVER002"	Dual network capability but only one cabled	Risk = medium: loss of ICZ Unicentre DSM if switch fails.	Cable 2nd nic to alternate switch	Change window only. Alternate switch port already available.
9	ICZ (WMQI): "SERVER003"	Dual network links but both patched to same switch.	Risk = low: loss of software upgrade capability only.	Re-patch 2nd nic to alternate switch	Change window only. Alternate switch port already available.
10	PZ (P590 switches): "SWITCH002"/ "SWITCH003"	Powered from single circuit. Only one circuit available to rack.	Risk = high: Loss of P590 PZ network connectivity if circuit trips.	Provide new circuit and re-power switch from new circuit.	Requires new power circuit to be run estimate 3-4 weeks.
11	PZ (Main switch stack)	Powered from single circuit. Only one circuit available to rack.	Risk = high: Loss of PZ network connectivity (including mainframe) if circuit trips.	Provide new circuit and re-power switches 1,3 and 5 from new circuit.	Requires new power circuit to be run estimate 3-4 weeks.
12	PZ (E-Dir switch):	No redundant uplink.	Risk = medium: Loss of	Connect cross-over from switch	Change window only.

			Novelle E-directory service if network uplink fails.	to main stack to provide alternate path.	
	"SWITCH004"				
13	PZ (E-Directory): "SERVER004" "SERVER005"	Both servers have dual power supplies but all 4 powered from same circuit	Risk = medium: Loss of Novelle E-directory service if power circuit trips.	Re-power redundant PSU's from ACS2 2-9	Change window only. Circuit already available.
14	PZ (E-Directory): "SERVER004" "SERVER005"	Both servers have dual network links but all 4 connected to same switch	Risk = medium: Loss of Novelle E-directory service if there is a network failure.	Re-patch 2nd nic's to alternate switch	Change window only. Alternate switch ports already available.
15	PZ (mainframe): AC01	Has dual network links but there is no auto failover configured.	Risk = high: Loss of mainframe connectivity if primary network link fails.	Investigate re-configuring options to enable full auto failover.	2 April
16	SGE Server:	Single network link to SGE DMZ	Risk = high: Loss of CMR access for external government agencies.	Server to be replaced with dual redundant nodes	End of May