Senate Economics Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Budget Estimates, 31 May to 2 June 2005

Question: Bud 8

Topic: **JCPAA Inquiry into the Management and Integrity of Electronic Information**

Hansard Page: **Written**

Senator Lundy asked:

1. Has Treasury complied with the recommendations accepted by the Government arising out of the JCPAA Inquiry into the Management and Integrity of Electronic Information in the Commonwealth Report? http://www.aph.gov.au/house/committee/jpaa/electronic_info/report.htm

2. If so, please itemise the activities that constituted compliance.
If not, provide specific details regarding the recommendations not complied with and why.

3. I ask the Department to provide an update (the years 03/04 and 04/05 to date) on the number of laptop computers, mobile phones and any other IT-related hardware that have been lost or stolen? Please provide disaggregated figures and the action that was taken?

4. I ask the Department to provide a list of all incidences notified on the ISIDRAS (DSD security incident reporting system) including the level notified.

Answer:

1 & 2

Recommendation 1
Treasury continues to receive annual accreditation to the Protected level of its computing environment. This review is performed by Defence Signals Directorate (DSD). Physical security plans for all information technology systems are updated progressively throughout the year and reviewed by DSD as part of the accreditation process.

Recommendation 2
Treasury has not outsourced any information technology services.

Recommendation 3

All recommendations are complied with through existing processes, policies and governance.

Recommendation 4

In house Asset Registers are maintained regularly and reconciled against quarterly equipment leasing payments and equipment schedules. Regular stocktakes are performed in support of this process and the preparation of the annual Treasury Financial Statements.

Recommendation 5

Complies.

Recommendation 6

Security risk management strategies are updated progressively and reviewed annually by DSD as part of the accreditation process and ANAO during their audits relating to the preparation of the annual Financial Statements.

Recommendation 7

Complies. Treasury has implemented TRIM Context software for the management of electronic documents and records. National Archives of Australia (NAA) has approved the Treasury Business Classification Scheme definitions and Disposal Authorities for the archiving or destruction of records. Treasury continues to develop and implement knowledge management strategies relating to all Treasury business and intellectual property.

Recommendation 8

Treasury has prepared Disaster Recovery Plans for all information technology infrastructure including networks and electronic storage equipment. Business Continuity Plans have also been prepared for all electronic information systems and IT applications. All plans are updated progressively and reviewed annually by DSD and ANAO.

Recommendation 9

Treasury does not use Gatekeeper.

3. There have been 9 lost or stolen mobile phones. The following is a list of all phones:

Phone number	Model	Incident	Incident report complete d.	Date of report to carrier	Sim card and IMEI blocked, new sim card issued
0412 356 243	Nokia	Lost	no	06/05/04	yes
0411 409 020	Nokia	Lost	no	01/09/04	yes
0421 612 567	Nokia 3530	Stolen	yes	30/11/04	yes
0412 627 101	Nokia 6610	Lost	no	14/12/04	yes
0419 224 644	Nokia 6610	Lost	no	20/12/04	yes
0418 613 071	Nokia	Lost	no	08/02/05	yes
0437 856 657	Nokia 3120	Lost	no	16/03/05	yes
0437 857 928	Nokia 3120	Stolen	yes	29/03/05	yes
0412 628 346	Nokia	Lost	no	21/04/05	yes

Treasury policy requires all stolen or damaged equipment to be reported to the CFO via an incident report. Both Stolen phones had been reported.

The sim card and IMEI are immediately blocked on all lost or stolen mobiles and new sim cards issued by the carrier.

During the 03/04 period one laptop computer and associated peripherals was destroyed in a house fire. There have been no equipment losses to date during the 04/05 period.

4. Treasury produces a level 2 ISIDRAS report each week covering the extensive unsuccessful port-scan hacking activity that occurs at the Internet Gateway during the preceding week. This report includes extensive text-based log files which DSD use for diagnostic purposes.

In addition to this standard reporting there have been two other ISIDRAS reports submitted to DSD.

1. A level 2 ISIDRAS report was submitted on 18 August 2003 and related to the infection of a laptop computer while connected to the Internet with the

W32.Welcha.Worm. The user reported the incident to IT Help Desk and the virus was resolved prior to connection of laptop to Treasury Network.

2. A Level 3 ISIDRAS report was submitted on 3 December 2003 and related to the infection of a laptop computer while connected to the Internet with a variant of the W32.Welcha.Worm. The offending laptop had not been connected for some time and did not have latest anti-virus definition files. The infected laptop was connected via remote access to the Treasury network and infected several servers. The virus did not spread further as all Workstations had current anti-virus definition files. Problem occurred and was resolved within the same day.