

Senate Economics Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Treasury Portfolio

Supplementary Budget Estimates

2016 - 2017

Division/Agency: Australian Bureau of Statistics

Question No: 27

Topic: 2016 Census – capacity testing / Distributed Denial of Service attacks

Reference: Written

Senator: Ketter, Chris

Question:

- 1) The Census is a high-profile, national endeavour that would make it a likely candidate for a Distributed Denial of Service attack. Why was such a huge amount of traffic not accounted for in capacity testing?
- 2) We're informed that the Census was capable of receiving [225 submissions per second], and was receiving 150 submissions per second at its peak. Were submissions per second the only type of load capacity tested?
- 3) What other scenarios of high demand – including denial of service attacks – were tested?
- 4) Did another contractor such as NextGen offer services such as those required to fend off a Distributed denial of service attack?

Answer:

- 1) The Australian Bureau of Statistics (ABS) had clearly stated requirements that the solution must be able to withstand DDoS attacks – along with other application based attacks.

As noted in the ABS Submission to the Senate Inquiry (page 62) : The ABS undertook a range of testing and independent assurance of the IBM developed and hosted online Census system.

Testing was undertaken to ensure that the expected volume of responses were able to be processed by the eCensus solution. In addition testing was undertaken to understand the absolute limits of the solution, this testing indicated that the eCensus solution was able to handle a peak load of 1.5 times the expected load.

The ABS did not independently test the DDoS protections that IBM was contracted to put in place, as it considered that it had received reasonable assurances from IBM.

The MacGibbon Review found IBM failed to implement adequate DDOS attack mitigation measures and that the ABS and IBM should have conducted additional and more thorough testing of the implementation of DDOS prevention measures.

- 2) The 2016 Census was rated to support 250 submissions per second and this figure was one determined through modelling of the peak load required to support 80% of Australian households completing their Census online. The load testing of the Census platform simulated users logging into the form, filling in the form (with save points in the form occurring at set stages) and then completing and submitting the form. The load testing also

included a percentage of users browsing the online help documentation, as well as submitting online inquiries.

- 3) Please refer to the ABS Submission to the Senate Inquiry - section 8.3 page 57 and to Online Census page 62.

The ABS tested that the platform could support and exceed the expected peak load of valid users.

ABS undertook failover testing. Failover testing involves deliberately causing parts of the infrastructure to fail under peak load to ensure that the system continues to function on the remaining infrastructure. Fail over tests included failing over to use only a single ISP network connection, failing a router, a web server, an application server, and a database.

The ABS tested the overload control mechanism. This mechanism is designed to be enabled if the platform experiences higher user load than anticipated. When invoked, this allows existing users to complete their form, whilst new users are given a message to try again soon.

For DDoS testing : on 5 August 2016 IBM undertook live testing of 'Island Australia' and informed the ABS that it had worked exactly as expected.

- 4) No contractor or vendor made any additional offers to the ABS regarding DDoS protection.