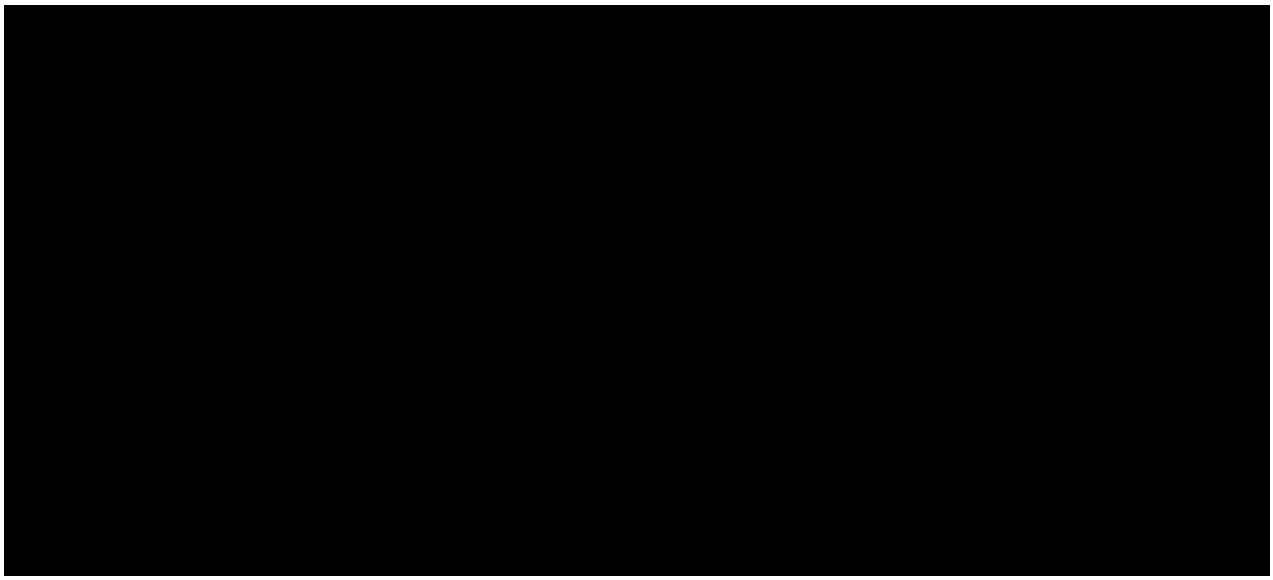
SENATE STANDING COMMITTEES ON ECONOMICS

INQUIRY INTO THE PREPARATION, ADMINISTRATION AND MANAGEMENT OF THE 2016 CENSUS BY THE AUSTRALIAN BUREAU OF STATISTICS

SUBMISSION OF IBM AUSTRALIA LIMITED

1. This submission is provided by IBM Australia Limited (**IBM**) to assist the Senate Committee inquiry and addresses paragraphs a. to e. of the Terms of Reference.



Executive summary

3. IBM was appointed by the Commonwealth (represented by the ABS), following a request for tender (**RFT**) process in 2014, to develop, implement and host the eCensus platform and application (i.e. the website and the electronic Census form) for the 2016 Census.

4. The contractual arrangements require the eCensus site to be available to the public to access, complete and submit electronic Census forms for a minimum of 98% of the 61 day period from 9.00 am on 26 July 2016 to midnight on 25 September 2016, as well as for 98% of the four hour peak period from 7.00 pm to 11.00 pm on 9 August 2016, being Census Day. The platform is also required to be able to handle form submissions at defined rates per second.

5. The eCensus site was made available to the public from 26 July 2016, as required. On 9 August 2016, the eCensus site was subject to four distributed denial of service (**DDoS**) attacks. (A brief, technical explanation of a DDoS attack is, for ease of reference, set out at paragraphs 61 to 64 of this submission.) As a result of the last of these attacks, which commenced at 7.27 pm, public access to the site was temporarily suspended - initially for approximately 3 hours at the direction of IBM, and immediately thereafter for

[1] Communications Management Plan v1.1 (Online Census 2016/03-002), paragraph 3.6.

approximately an additional 40 hours at the direction of the ABS.

6. IBM deeply regrets the inconvenience that has been caused to the Australian public and the Government by reason of the eCensus site not being accessible during the period it was temporarily unavailable.

7. No Census data was exfiltrated as a result of any of the DDoS attacks. IBM has investigated the matter and the ABS and the Australian Privacy Commissioner have separately confirmed the position. (See paragraphs 102 to 109 below.)

8. IBM had anticipated and planned for the risk of DDoS attacks to the eCensus site. The main defence mechanism utilised was a form of protection known as geo-blocking (known internally at IBM as "Island Australia"). In short, the geo-blocking arrangement involves blocking or diverting international traffic intended for the eCensus site before it reaches the site, while leaving the system free to continue to process domestic traffic. This method was chosen because the primary risk of DDoS attacks of sufficient size to disrupt site availability was considered to be from foreign sources.

9. Data security is of paramount importance to IBM, as it is to the Australian Government. IBM included a number of data security features in the design solution that it developed and implemented for the eCensus site, which provide multiple layers of protection. The Australian public has no reason to fear that personal information was exposed. The loss of availability of the eCensus site on 9 August 2016 was, of course, deeply regrettable; but it should be stressed that the issue was a temporary availability problem, and not a data security problem.

10. Public access to the eCensus site is provided via two internet service provider (**ISP**) links. One is provided by NextGen Networks Pty Ltd (**NextGen**) and the other by Telstra Limited (**Telstra**). The geo-blocking arrangements are implemented by the ISPs at the direction of IBM. When a DDoS attack is attempted, and is sufficiently severe so as to warrant implementing the geo-blocking arrangement, IBM directs NextGen and Telstra to put Island Australia into place. (See paragraphs 65 to 78 below.)

11. Both prior to, and during, the course of the operations of the project, information about the eCensus site defence arrangements was treated as confidential and generally shared only on a need-to-know basis to ensure site security. The ABS and the Australian Signals Directorate (**ASD**) were aware that IBM intended to use geo-blocking. The ABS' IT Security personnel considered geo-blocking to be an "extremely effective control".[2] IBM understands that the ASD was asked by the ABS to review the security arrangements for the 2016 eCensus site, but the ASD declined to undertake a detailed review. (IBM understands that the ASD had reviewed arrangements for the 2011 Census, which also employed geo-blocking arrangements.) That said, IBM and the ABS

[2] See the document titled "ASD Recommendations and Advice", authored by [redacted] (IT Security, ABS), p 12 which states: "*Another extremely effective control in place is the ability to only accept traffic from Australia, if an attack is detected (although using a non-traditional method of geoblocking). Any global botnet is unlikely to have a significant enough number of nodes residing in Australia to continue an attack*." See also paragraph 72 below.

met with the ASD on 21 July 2016 to seek its input on security threats for the project. During the course of that discussion, IBM asked the ASD if it was aware of any intelligence relating to planned denial of service attack risk. The ASD said it was not and that it would keep the ABS/IBM informed if such intelligence emerged. The ASD did not provide IBM with any such intelligence. IBM is also aware that the ABS met with the Australian Security Intelligence Organisation on 21 July 2016 to discuss security issues relating to the project, but is not aware of what was discussed.

12. At 7.27 pm on 9 August 2016 (Census Day), a DDoS attack (the fourth of the day) was detected by IBM on the eCensus site. The attack was of significant size and had the effect of causing the site to become unresponsive and unavailable to the public as described below. The attack was foreign-sourced and hit the eCensus site via the NextGen link at a time when IBM had already directed NextGen (and Telstra) that Island Australia was to be in place and in circumstances where NextGen had provided repeated assurances to IBM prior to the attack that it had done so.

13. In fact, the assurances were incorrect. IBM was informed - later that day after the attack had passed - that a Singapore link operated by one of NextGen's upstream suppliers (Vocus Communications or **Vocus**) had not been closed off and this was the route through which the attack traffic had entered the NextGen link to the eCensus site. Vocus admitted the error in a teleconference with IBM, NextGen and Telstra around 11.00 pm on 9 August 2016. (See paragraphs 92 to 96 below.)

14. Had NextGen (and through it Vocus) properly implemented Island Australia, it would have been effective to prevent this DDoS attack and the effects it had on the eCensus site. As a result, the eCensus site would not have become unavailable to the public during the peak period on 9 August 2016.

15. IBM accepts its responsibility as head contractor for the eCensus project. NextGen was a service provider to IBM. IBM simply notes that the use of ISPs to provide links to a website such as the eCensus site is required for such projects and cannot be avoided.

16. The site underwent performance and security testing by the ABS (including via its testing contractors) before it went live. IBM also performed hundreds of tests itself in the course of developing the site and the eCensus application. The geo-blocking arrangement was tested prior to Census Day and worked. A geo-blocking arrangement had also been implemented as a DDoS defence for the 2011 Census.

17. Regrettably, the 7.27 pm DDoS attack also caused one of the mechanisms used by IBM to monitor the performance of the eCensus site to miscarry. As a result, some IBM employees who were observing the monitor mistakenly formed the view that there was a risk that data was being exfiltrated from the website and that the risk needed to be further investigated. Out of an abundance of caution, IBM shut down access to the site and assessed the situation. The cause of the problem was identified. No data exfiltration occurred.

18. A further consequence of the 7.27 pm DDoS attack was that the firewall to the eCensus site - through which IBM's control link to the routers on both the NextGen link and the

Telstra link operated - became overloaded with data. The overload of the firewall required manual rebooting of an IBM router on the open Telstra link which, due to a configuration error, took approximately 1 hour and 20 minutes to resolve.

19. By 10.32 pm on 9 August 2016 - approximately 3 hours after the start of 7.27 pm DDoS attack - IBM had rectified the issues that had caused the eCensus site to become unresponsive and, accordingly, informed the ABS that it was ready to make the site available to the public again. At that point, IBM was instructed by the ABS not to do so while checks being undertaken by the ABS and ASD were completed. At the direction of the ABS, public access to the eCensus site was restored at about 2.30 pm on 11 August 2016 (approximately 40 hours later).

20. Of the 1,479 hours that the eCensus site is due to be available to the public (over the 61 day, 15 hour period from 26 July to 25 September), it is anticipated - at the time of submission of this document - that the site will have been available for approximately 1,436 hours, or 97.1% of that period. IBM accepts that, as a result of the sequence of events following the 7.27 pm DDoS attack, it did not make the eCensus site available for 98% of the four hour period from 7.00 pm to 11.00 pm on 9 August 2016.

21. As at the date of writing these submissions, there have been further DDoS attacks on the eCensus site since 11 August 2016. They have all been successfully defended. As the site is still operational, it is not intended to discuss these further in this submission for operation security reasons.

22. IBM is one of the world's largest IT services consulting firms. It has a strong commitment to Australia. IBM has conducted business in Australia for 84 years, it has a long relationship with the Australian Government as a client, and it has undertaken many hundreds of projects successfully and to the mutual benefit of both parties. IBM successfully delivered both the 2006 and 2011 eCensus projects. The 2006 eCensus project received a number of awards.[3]

23. The DDoS attacks on 9 August 2016 highlight the importance of the risk that cybersecurity threats present to both government and industry, now and into the future. The use of electronic platforms for projects like this - and more generally - will increase into the future. In 2006, the eCensus response rate was 9%. In 2011, it increased to 33%. The ABS indicated on 2 September 2016 that the collection of Census data was proceeding "ahead of schedule".[4] As at the date of this submission, IBM understands that approximately 59.2% (as at 12.00 midnight on 20 September 2016) of Australian households who have completed their Census have used the eCensus site to submit their Census information. (A final, updated figure will be provided once the eCensus site

[3] The 2006 eCensus won the 2007 e-Government Award for being the most outstanding successful project of the year in the delivery of e-government services to business, citizens and the community (see ABS Media Release, 7 May 2007, "ABS eCensus wins Award for Excellence in Government"). The 2006 eCensus was also listed in the Laureates Class of 2007 by the Computerworld Honors Program, an international program recognising visionary applications of information technology that benefit society (see the Computerworld Honors Program, "Laureates Class of 2007").

[4] Article titled "Census returns now topping 80 per cent" authored by Rachel Baxendale (The Australian) (3 September 2016).

closes on 25 September 2016.) At the same time, DDoS attacks - which are only one form of cybersecurity risk - can also be expected to occur with greater frequency and intensity into the future.

24. In terms of improving the design of the eCensus (and similar projects) going forward, IBM offers the following observations and suggestions in relation to DDoS attacks (which are not intended as a criticism of any government agency or the approach taken on this occasion to the Census):

    (a) the risk of DDoS attacks needs to be assumed. For high profile projects like this one, it should be expected that DDoS attacks will be increasingly attempted. No DDoS attacks occurred on the eCensus site in 2011 or 2006. This suggests that other factors were in play in 2016 to make the site a target of greater interest to potential attackers. Those factors might be investigated;

    (b) the motivations of those launching DDoS attacks can include attracting attention and causing maximum disruption. The risk of disruption is more pronounced when there is a short maximum peak period of legitimate traffic; and

    (c) in the present case, the eCensus site will, by project end, have been open for approximately 61 days. It is possible that many Australians mistakenly formed the view from the Census advertising campaign that:

        i. the site was not open prior to Census Day; and

        ii. the public had to complete the Census online on 9 August 2016, rather than simply during the 61 day period the eCensus site was open.

    It is also possible that many Australians did not clearly understand that the Census Day is simply the reference point for the data required to be provided when completing the Census. As such, a different approach to the advertising for future Census projects to address these matters may be helpful to support an increased online submission rate. (For clarity, IBM has no role to play in the Census advertising campaign.)

25. IBM is a global leader on cybersecurity issues and sees Australia as an important voice in the Asia Pacific region on cybersecurity initiatives. IBM is currently developing a number of initiatives in Australia to further support the focus on the important challenge faced by all sectors in dealing with cybersecurity risk and to aid the development of cybersecurity solutions.

26. IBM is at present assisting the Australian Federal Police with its investigations into this matter. An attack of the present kind requires access to a significant botnet arrangement, and these are prevalent in an increasing number of foreign countries.

27. IBM is willing to appear before the Senate Committee if that would assist the Committee's work in relation to this inquiry.

FURTHER DETAIL RELEVANT TO TERMS OF REFERENCE

IBM and its previous engagements by the ABS for the 2006 eCensus and 2011 eCensus

28. The ABS has implemented online solutions for the past three Census cycles. The first use of an electronic form in combination with a paper form was to a limited number of households in 2001. This was followed up in 2006 and 2011 with an "eCensus solution" – being an electronic form or "eForm" that could be completed by respondents to the Census online by interacting with an ABS website as an alternative to completing the paper form (**2006 eCensus** and **2011 eCensus**).[5]

29. IBM was engaged by the ABS to provide IT services in relation to the 2006 eCensus and 2011 eCensus.[6] IBM developed the electronic form and the online hosting environment (known as a "platform" or "system"). The solutions provided by IBM were successful, and saw the percentage of respondents who completed the electronic form rather than the paper form (the "online response rate") increase from approximately 9% in 2006 to 33% in 2011.[7]

30. An ABS review after the 2006 eCensus concluded that the solutions provided by IBM had delivered 100% availability through the Census' busiest period, from Saturday, 5 August to Sunday, 13 August 2006. Average page response times remained below one second within the IBM environment.[8]

31. For the 2011 Census, IBM delivered 100% availability through the Census' busiest period – from Saturday, 6 August to Sunday, 14 August 2011. Approximately 200,000 households were using the system at the peak time of 8.43 pm on Tuesday, 9 August 2011, achieving 85 eCensus submissions per second. Average page response times remained below one second within the IBM environment.[9]

32. In 2014, the ABS described the online solutions provided by IBM for the 2006 eCensus and 2011 eCensus as "very successful".[10]

33. Apart from supporting the eCensus in 2006, 2011 and 2016, IBM was also engaged in each of those Census cycles (and in 2001) to provide to the ABS an IT service whereby information in the paper forms completed by respondents was converted into electronic form and processed into an electronic database (known as the "Paper Data Capture Solution"). This work was tendered for, and contracted, separately from the work related to the eCensus in 2006, 2011 and 2016.[11]

---

[5] Statement of Requirements for 2016 eCensus Solution, ABS2014.105 (**Statement of Requirements**) at [1.2].
[6] Response to RFT, pp 1-4.
[7] ABS, Census Update, October 2006, Issue 40, p 6 and Statement of Requirements at [1.4].
[8] ABS, Census Update, October 2006, Issue 40, p 6.
[9] IBM News Release, 27 September 2011, "IBM helps Australian Bureau of Statistics break records with the 2011 Census".
[10] Statement of Requirements at [1.2].
[11] Most recently, IBM and the Commonwealth (represented by the ABS) entered into a contract dated 27 September 2013 for the provision of software licences, maintenance and support for the Paper Data Capture

The 2016 RFT

34. On 25 July 2014, the ABS issued a Request for Tender for IT services related to the 2016 eCensus (**2016 RFT**), including a Statement of Requirements.[12] The Statement of Requirements indicated that the approach to be adopted for the 2016 eCensus was to build on the solution provided by IBM in 2006 and 2011 (which had been adapted by the ABS in the period up to 2014) with the aim of increasing the online response rate for the 2016 eCensus to 65%:[13]

> A key focus of the 2016 Census is to make it easier for the public to respond while delivering a more efficient and effective Census. We will offer the eCensus to all households (approximately 10 million) with the aim of increasing the on-line response rate from 33% achieved in 2011 to 65% in 2016.
>
> To meet the overall objective of the 2016 Census the ABS has recognised the need for a Prime Partner to work with the ABS on the continued development of the existing eCensus solution and to host the eCensus.
>
> The use of the previously developed 2011 eCensus solution is required to minimise change to Census processes, reducing risk and time delays. A number of Census applications have been developed which integrate tightly with the existing ABS eCensus solution. Since 2011 the ABS has continued to develop the eCensus solution on an Oracle platform and added features in to the application which the ABS will want to include moving forward.

35. The Statement of Requirements described the "Outcome Sought" by the ABS in the following terms:[14]

> The ABS requires the Prime Partner to use the 2011 eCensus Application as the main building block for the 2016 eCensus. The ABS has undertaken further development of the 2011 Application and prototyped a number of features which are included in the 2014 Application and will be required to incorporate in the 2016 eCensus Application.

36. The Statement of Requirements also set out the ABS' overall "Business Requirements" as follows:[15]

> The following is a list of business requirements which may be met in a variety of ways depending upon the implementation of the solution, with the value for money consideration an overarching requirement. The solution will be tested against these items to assess the technical merits of meeting ABS objectives.

Solution for ABS surveys and the 2016 Census. The contract period is 1 July 2013 to 30 June 2018 and the contract value is $1.6 million, as recorded on the Government's AusTender website (ID: CN1870631-A1).

[12] Request for Tender for eForms Solution for the 2016 Census, pp 4-5.

[13] Statement of Requirements at [1.4]-[1.6].

[14] Statement of Requirements at [1.12].

[15] Statement of Requirements at [1.16].

a) **Security**

Information is secure and confidential, Secure Hosting environment, Encryption.

b) **Performance and Capacity**

High Availability, Scalability, Support for a variety of environments.

c) **Data Quality**

Validation, Authentication, Format.

d) **Accessibility & Usability**

Ease of access and use, Online Help, Resumable.

e) **Functionality of the form**

Navigation, Easy to complete, Sequencing, Individual responses.

37. The Statement of Requirements stated that the above requirements were listed in order of priority - that is, the highest priority was to be accorded to "Security", which involved ensuring that information was "secure and confidential".[16]

38. To achieve the stated requirements, the ABS required the tenderer to work to a particular timeline, the key elements of which were described as the "Dress Rehearsal", the "Main Event", the "Census Night" and the "Census Night Peak Period".

39. There appears to have been a misunderstanding in sections of the media that the 2016 Census was required to be responded to on Census Night and that the 2016 eCensus was, at least initially, only intended to be accessible on Census Night. That has never been the case. Census Night is the temporal reference point to be applied by respondents when providing information as part of the Census. However, it has never been intended that respondents would be restricted to completing the electronic form on Census Night only. As is apparent from the terms of the Statement of Requirements, there was always to be a period of about two months during which the 2016 eCensus was required to be "live" so that respondents could access, complete and submit the electronic form.

40. The Statement of Requirements included specific requirements relating to availability. It stated:[17]

> The Application must be available for Respondents to complete their Census form for the 2015 Dress Rehearsal (60,000 households) and for 2016 Main Event (10,000,000) households.
>
> The Application must be available 24 hours a day, 7 days a week for

[16] Statement of Requirements at [1.8].
[17] Statement of Requirements at [4.3]-[4.4].

respondents to complete their Census form during the Dress Rehearsal and Main Event periods. The Application must have following minimum availabilities;

a) 98% during the 2015 Dress Rehearsal Period

b) 98% for 2016 Main Event Period excluding Census night peak period and

c) 98% during the Census Night Peak Period (1900-2300 AEST).

41. IBM's performance against these availability specifications is set out in paragraphs 98 to 101 below.

IBM's Response to RFT and the 2016 Contract

42. On 22 August 2014, IBM submitted a response to the 2016 RFT (**Response to RFT**).[18]

43. IBM proposed that the project team for the 2016 eCensus would "form around a core team that [has] worked with the ABS for eCensus in 2006 and 2011".[19]

44. IBM was selected by the ABS and in September 2014 a contract was entered into (**2016 Contract**).[20] The 2016 Contract is for a period of 25 months (from 1 October 2014 to 31 October 2016).[21]

45. The services to be provided by IBM under the 2016 Contract are extensive. In summary, they consist of:[22]

(a) preparing detailed design documents including Application Design and System Architecture documents, to be approved by the ABS;

(b) preparing a detailed Project Plan document, to be approved by the ABS;

(c) preparing detailed Risk Management and Communication Plan documents, to be approved by the ABS;

(d) preparing detailed Acceptance Process Plan and Test Plan documents, to be approved by the ABS;

(e) managed services, in the form of developing, implementing and hosting the "eCensus System" to specified Service Levels, including the provision of a full hosting

[18] See letter dated 22 August 2014 from Ms Permenthri Pillay, IBM, to Ms Helen Robson, ABS, enclosing a document titled "Response for the Provision of Services for the eCensus Solution – RFT Ref: ABS2014.105".
[19] Response to RFT, p 11.
[20] Agreement between the Commonwealth of Australia represented by the Australian Bureau of Statistics and IBM Australia Limited in relation to Services for eCensus and Data Capture Solution ABS2014.105.
[21] 2016 Contract, p 64 (Appendix 1).
[22] 2016 Contract, pp 64-74 (Appendix 1), and see also the list of Project Deliverables at pp 76-77 (Attachment 1 to Appendix 1).

environment (hardware and software);

(f) testing, reviewing, reporting on and refining the eCensus System; and

(g) making the eCensus System available during the periods specified in the contract.

46. The 2016 Contract included a project timetable, which slightly adjusted the timing that had been contemplated in the 2016 RFT.[23] In particular:

(a) the Dress Rehearsal was to take place between 21 July 2015 and 31 August 2015; and

(b) the Main Event was to take place from 26 July 2016 to 5 September 2016 inclusive.

47. Consistent with the RFT, the 2016 Contract required IBM to make the electronic form available to be accessed and completed by respondents online during the "Main Event".[24] In other words, the electronic form was to be made available from 26 July 2016 to 5 September 2016 and not only on 9 August 2016, being the Census Day. (This was later extended to 23 September 2016, and more recently to 25 September 2016. See paragraph 51 below.)

Performance of the 2016 Contract

48. In or about February 2015, the ABS informed IBM that it was considering not proceeding with the 2016 eCensus (or, indeed, any Census in 2016). IBM understands that the ABS was considering decreasing the frequency of the Census to once every 10 years and running a rolling Australian Population Survey (**APS**) during the intercensal period. IBM was asked to provide a set of quotations for a range of options for re-purposing the 2016 eCensus solution to support the APS. These quotations were developed during March and April 2015, pursuant to a Change Order.[25] As part of that Change Order, the ABS and IBM agreed that if the 2016 Census were to proceed, then the Dress Rehearsal would occur in October 2015 and the Main Event would occur in October 2016.[26] In May 2015, the ABS informed IBM that the existing 5 yearly Census frequency would be maintained and the 2016 eCensus would proceed, with Census Day to be 9 August 2016 as originally planned.

49. The consideration given by the ABS to abandoning the 2016 Census from about February to May 2015 resulted in a delay to the timing of the 2015 Dress Rehearsal. The 2015 Dress Rehearsal initially required by the ABS was replaced by a "Self Response Test" (as a result of agreed revisions to eCensus program activities) which had a reduced scope and removed dependencies on field enumeration operations.[27] As such, the contract was amended to eliminate the requirement for the Dress Rehearsal on 21 July 2015 (or at all). It was agreed that the Self Response Test would be held from 20 August to 21 September

[23] 2016 Contract, pp 76-77 (Attachment 1 to Appendix 1).
[24] 2016 Contract, p 85 (Attachment 4 to Appendix 1).
[25] Change Order ABS2014.105-004.
[26] Change Order ABS2014.105-004.
[27] Change Order ABS2014.105-010 (approved by both IBM and the ABS on 25 September 2015).

2015.[28]

50. In about October 2015, following the Self Response Test, the ABS requested that IBM increase the eCensus hosting infrastructure capacity to support an online take-up of 80% (rather than the 65% initially agreed). This was documented as a formal change to the 2016 Contract and implemented by IBM.[29]

51. In May 2016, the 2016 Contract was further varied to extend the agreed Main Event end time from 5 September to 23 September 2016.[30] As a result of the events of 9 August 2016 a further extension has been made to 25 September 2016.[31]

52. All of the documents required to be prepared by IBM to date and approved by the ABS under the 2016 Contract have been prepared and approved. The Self Response Test was held in August and September 2015 as stipulated and the results of this test were documented.[32]

53. IBM developed the "eCensus system" called for by the 2016 Contract and provided a hosted environment in the form of a dedicated physical environment composed of individual servers in dedicated security racks in IBM's data centre at Baulkham Hills NSW. The electronic form was able to be accessed, completed and submitted online by respondents from 26 July 2016 and, subject to the loss of availability incident on 9 August 2016, will continue to be available until 25 September 2016. As set out further below, the eCensus system was subject to an extensive testing regime by the ABS (and the contractors it engaged), including in relation to the performance of the system.

54. IBM is not aware of any issue concerning its delivery of the above services other than loss of availability of the eCensus on 9 August 2016.

Testing of the eCensus system

55. The 2016 Contract provided for extensive testing activities to be undertaken by the ABS, as well as some testing activities to be undertaken by IBM and others to be undertaken jointly by the ABS and IBM.

56. The testing activities to be undertaken by the ABS were:[33]

    (a) User Acceptance Testing (to verify the functional behaviour of the eCensus system against its specifications);

    (b) accessibility testing (to verify the conformity of the eCensus site to its accessibility requirements);

    (c) useability testing (to evaluate the useability aspects of the eCensus system to ensure

[28] Production Performance Analysis – Dress Rehearsal v1.0 (eCensus 2016/08.2-028) at [2.1].
[29] Change Order ABS2014.105-069.
[30] Change Order ABS2014.105-014 (approved by IBM on 19 May 2016 and the ABS on 24 May 2016).
[31] Change Order ABS2014.105-093.
[32] Production Performance Analysis – Dress Rehearsal v1.0 (eCensus 2016/08.2-028).
[33] 2016 Contract, pp 102-104 (Attachment 8 to Appendix 1).

they meet the ABS requirements);

(d) penetration testing including Web Application Security Testing (to check the operational security of the eCensus system against web-based attacks);

(e) a security (IRAP) assessment (to evaluate the security design of the eCensus system);

(f) ABS infrastructure load testing for the processing systems receiving respondent data;

(g) contractual compliance performance testing (to verify that the eCensus system could support its key performance criteria); and

(h) testing of the Notice of Direction System.

57. The 2016 Contract required IBM to prepare a detailed Test Plan for approval by the ABS. In compliance with that obligation, IBM developed a Master Test Plan that was approved by the ABS on 8 May 2015 (the **Master Test Plan**).[34] The Master Test Plan confirmed the allocation of responsibility for the activities set out at paragraph 56(a) to (h) above to the ABS, save in respect of the security (IRAP) assessment, which was not referred to expressly in the document but remained at all times the responsibility of the ABS.[35] The Master Test Plan did, however, contain an extract from the 2016 Contract that lists IRAP under Customer activities.

58. IBM is aware that the ABS engaged external contractors to assist it in conducting certain testing activities which were the responsibility of the ABS, namely:

(a) UXC Saltbush, to undertake two different types of testing: code review and penetration testing. No issues of significance emerged in the course of either testing program; and

(b) Revolution IT, to undertake several kinds of performance testing (stress testing, soak testing and failover testing). This was designed to verify the capability of the eCensus system to process the load expected to be generated during the peak Census period on 9 August 2016 (which was 250 Census response submissions per second). Revolution IT has stated publicly that "[t]he performance testing completed by [it] was successful and no evidence suggests that there was a performance issue as a result of legitimate users accessing the site".[36]

59. IBM was responsible for undertaking certain other types of testing including system, performance and volume testing. These included tests designed to verify that the eCensus system met its committed response time and could process the required number of submissions. The issues that emerged during the testing undertaken by IBM were addressed.

[34] Master Test Plan v1.1 (eCensus 2016/08.3-002).
[35] Master Test Plan v1.1 (eCensus 2016/08.3-002), pp 15-17.
[36] Revolution IT Media Release, titled "Revolution IT Q and A – Australian Bureau of Statistics (ABS) 2016 Census Website".

IBM's planned response to DDoS attacks

60. The Statement of Requirements stated that "[t]he hosted environment must be protected from Distributed Denial of Service (DDoS) attacks, particularly during the peak collection period".[37] As explained below IBM proposed to meet that requirement by use of a geo-blocking procedure (referred to within IBM as "Island Australia").

Denial of service attacks

61. A denial of service attack is a malicious attempt to make a system unavailable to its intended audience by overloading servers with requests to render it unavailable or causing it to shut down.

62. A denial of service attack is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

63. A "distributed" denial of service or DDoS attack occurs where the attack source has multiple unique IP addresses or "nodes". It is typically achieved by using a "botnet", being a group of internet-connected devices on which malware has been installed so as to enable the devices to be controlled from a remote location without the knowledge of the devices' owners. A DDoS attack may be regarded as analogous to a group of people crowding the entry door to a business and not allowing legitimate customers to enter, thus disrupting the business' normal operations.

64. The effects of denial of service attacks include slower network performance (opening files or accessing websites), or the unavailability of a particular website, or an inability to access any website. Denial of service attacks are therefore directed towards the performance or availability of a website. Of themselves, they do not involve illicitly acquiring information from the website (although, of course, the persons who carry out such attacks may attempt to acquire information by other means).

Rationale for the Island Australia protocol

65. IBM's planned response to DDoS attacks was through the implementation of the Island Australia protocol. The protocol was an ISP-based DDoS attack mitigation strategy which required the ISPs who provide access to the eCensus site to block or divert all international traffic to the site at the direction of IBM. Such blocking is known as "geo-blocking". The protocol was to be deployed in the event that a DDoS attack occurred.

66. The Island Australia protocol, while not a form of protection that is appropriate for websites with users who are widely distributed, was well-adapted to the 2016 eCensus because it took advantage of the fact that the Census form was required to be completed (during the Census period) only by persons who, on the Census Day, were physically present in Australia. Accordingly, with some exceptions,[38] legitimate traffic to the

[37] Statement of Requirements at [7.19].
[38] The reason why it is not appropriate to permanently block international traffic is that some Australian users will have arrangements in place such that their access to the eCensus website is via an international IP address.

eCensus site could be expected to be domestic to Australia.

The role of ISPs

67. An ISP is an organisation that provides services for accessing and using the internet. IBM engaged Telstra and NextGen to provide ISP services in relation to the eCensus. In the context of the 2016 eCensus, Telstra and NextGen provided the links through which data passed when the public sought to access the eCensus site. Both are leading ISPs who routinely provide ISP services to a range of Australian businesses, government agencies and telecommunications service providers. It is not possible for an IT services company such as IBM to implement the 2016 eCensus without engaging ISPs.

68. It was necessary for IBM to involve the ISPs in the implementation of the geo-blocking solution as they have control over their respective data networks and are in a position to block internet traffic originating from particular domains or IP addresses. IBM's engagement of ISPs was referred to in its Response to RFT.[39]

The development of the Island Australia protocol

69. The geo-blocking solution for denial of service attacks had been used by IBM as part of the 2011 eCensus and in that context was known to and approved by the ABS and ASD.

70. The proposed use of geo-blocking as needed for the 2016 eCensus site was foreshadowed by IBM in the Response to RFT[40] and the Risk Management Plan,[41] a document that IBM was required to prepare under the 2016 Contract for the ABS' approval.

71. The ABS was briefed on the operation of the geo-blocking solution at risk management workshops in 2014 and 2015.[42]

72. In March 2015, the ASD provided a series of recommendations and advice to the ABS for the 2016 eCensus. IBM's understanding is that a summary document of the ASD's review outcomes was prepared by [redacted], IT Security, ABS. The document contains the following observations in relation to the proposed use of a geo-blocking solution:[43]

> Another extremely effective control in place is the ability to only accept traffic from Australia, if an attack is detected (although using a non-traditional method of geoblocking). Any global botnet is unlikely to have a significant enough number of nodes residing in Australia to continue an attack.

[39] Response to RFT, p 6.
[40] Response to RFT, p 93.
[41] 2016 Online Census Risk Management Plan v1.8 (Census 2016/05-001), p 13 at [R033].
[42] This includes the risk management workshop in October 2014 in Ballarat.
[43] Document titled "ASD Recommendations and Advice", authored by [redacted] (IT Security, ABS), p 12.

Testing and implementation of Island Australia

73. The Island Australia protocol response plan involved the following elements:

    (a) IBM staff contacting Telstra and NextGen upon becoming aware of a DDoS attack to activate Island Australia;

    (b) Telstra and NextGen activating Island Australia (which could be achieved within 2 minutes);

    (c) establishing a conference bridge between IBM, Telstra and NextGen; and

    (d) IBM, Telstra and NextGen managing a coordinated DDoS attack response.

74. For security reasons, details of the proposed use of the geo-blocking response plan were only disseminated strictly on a "need-to-know" basis.

75. Telstra and NextGen agreed to block international traffic as a DDoS mitigation strategy. Their ability to block international traffic was confirmed and subsequently tested, with the ABS' consent, on 5 August 2016 at 6.00 am. The testing was successful, with the ISPs implementing the plan within 120 seconds of notification and international traffic being restored 10 minutes later. The testing of the strategy after the system had gone live and proximate to the Census Day had been raised with the ABS and was appropriate given that a limited number of responses were expected to be received before the Census Day. The ABS was informed of the outcome of the test by email report.

76. IBM considers that, following the testing on 5 August 2016, it had every reason to think that Island Australia would provide effective protection against DDoS attacks if needed.

77. For completeness, IBM considered other possible options for the defence of DDoS attacks. It also determined, in consultation with NextGen in the planning phase, that certain products would not be suitable for the 2016 eCensus because of the unique traffic profile it was expected to generate.

78. As such, IBM determined that geo-blocking was the most simple and effective DDoS attack mitigation strategy for the ABS' practical requirements. As explained below at paragraphs 92 to 96 there is no reason to doubt that had Island Australia been implemented properly on 9 August 2016 it would have been completely effective.

Events of 9 August 2016

79. On 9 August 2016, there were four DDoS attacks on the eCensus system. The first DDoS attack took place at 10.10 am and subsided by itself at 10.20 am. A second DDoS attack occurred at 11.45 am. IBM initiated the Island Australia protocol within 2 minutes of the start of the second attack by contacting the ISPs and directing them to perform the protocol. Traffic to the eCensus site returned to normal by 11.49 am.

80. At the direction of the ABS, IBM kept Island Australia in place following the second attack.

81. At 4.52 pm, there was a third minor DDoS attack which had no impact on the availability of the eCensus system. As Island Australia was in place, it was initially thought that the attack had been directed at the IP address of the User Acceptance Testing (**UAT**) environment which shares a firewall with the production environment. The UAT IP address was subsequently added to the IP addresses to which the Island Australia protocol applied so as to eliminate this possibility.

82. IBM also sought assurances from both Telstra and NextGen that the Island Australia protocol was correctly in place. Both ISPs confirmed that Island Australia had been properly implemented. IBM also sought assurance from NextGen that its upstream providers, NTT Communications (**NTT**) and Vocus, had implemented the Island Australia protocol correctly. NextGen gave assurances that NTT and Vocus had confirmed Island Australia was implemented.

83. At about 7.27 pm, there was a fourth DDoS attack. The fourth attack resulted in the system being overwhelmed. By 7.38 pm, the eCensus site was unresponsive and unavailable to users. It is now clear that the reason for the site becoming unresponsive and unavailable was that Vocus had failed to implement geo-blocking on one of its links through Singapore, which allowed the DDoS attack to occur via the NextGen link. This is addressed in more detail at paragraphs 92 to 97 below.

84. During the fourth attack, a system monitoring dashboard, which included a graph of inbound and outbound ISP traffic to the eCensus site, showed what appeared to be a spike in outbound traffic. This caused some IBM employees to, it is now accepted mistakenly, form the view that there was a risk of data egress from the eCensus site. In fact there was no data egress and the spike was a "false positive". That issue is addressed at paragraphs 102 to 109 below.

85. Acting conservatively, and in keeping with its understanding that maintaining the security of the data obtained in the 2016 eCensus was the ABS' paramount concern, IBM made the decision to activate the overload control, which had the effect of stopping the public from logging on to the eCensus site and accessing the form.

86. Once the overload control was enabled, an attempt to reboot the router at the IBM end of the NextGen link was made to regain logon access and traffic flow. The NextGen link remained down. The router at the IBM end of the Telstra link was also rebooted but the router failed to reload its configuration. This meant that both links were unavailable.

87. IBM worked to rectify the issues that had been created by the DDoS attack by disconnecting the NextGen link and reconfiguring the router on the IBM end of the Telstra link. The reboot on the router to the Telstra link router was due to an incorrect setting on that machine and this issue took approximately 1 hour and 20 minutes to resolve. IBM emphasises that the router on the Telstra link was owned by IBM and it takes responsibility for the configuration error with this piece of equipment. By about 10.30 pm on 9 August 2016, the platform had returned to its normal state and the eCensus site was in a position to be made available to the public again.

88. Immediately after this - being shortly after 10.30 pm on 9 August 2016 - IBM contacted

the ABS and informed it that IBM was ready to make the eCensus site available to the public by removing the overload control. IBM was directed by the ABS not to put the system back online until any prospect of data egress had been ruled out to the satisfaction of the ABS and ASD.

89. On 10 August 2016 at 2.00 am, there was a conference call between IBM, the ASD and the ABS. The purpose of the call was to brief the ASD on whether there had been any data egress as a result of the DDoS attacks. IBM informed the ASD and ABS that its investigations had confirmed there had been no data egress as a result of the DDoS attacks. At this time, the ASD and ABS took a conservative decision to keep the overload control in place until further notice (which meant only users already logged onto the eCensus system could submit responses).

90. IBM representatives met with representatives of the ABS and ASD on a number of subsequent occasions on 10 August 2016. At a meeting in the afternoon of 10 August 2016, the ASD informed IBM that it had been decided not to return the system to normal operation until IBM had provided a written report explaining what had occurred and confirming that there had been no data egress by 8.00 am on 11 August 2016.

91. IBM prepared such a document overnight on 10 August 2016, in the form of a "Census Day DDoS Event and Mitigation" document. The document was provided to the ABS and ASD as soon as possible on 11 August 2016. A meeting then took place between IBM, the ASD and the ABS. Following the meeting, at about 2.30 pm on 11 August 2016, IBM was instructed to remove the overload control, keep Island Australia in place, and make the system available to the public again and IBM did so.

Reasons why the eCensus site was temporarily unavailable

92. From the time that the DDoS attacks commenced on 9 August 2016, IBM was in frequent communication with the ISPs. In particular, there were numerous telephone calls between IBM and representatives of Telstra and NextGen in which the representatives of Telstra and NextGen assured IBM that Island Australia had been put in place and international traffic had been blocked.

93. At approximately 10.17 pm on 9 August 2016, NextGen provided the traffic log for the NextGen link for the period from 6.15 pm to 10.15 pm. The log showed that the NextGen link had been saturated for the duration of the fourth attack. At approximately 10.27 pm, Telstra provided its traffic log for the Telstra link. The log showed that the Island Australia protocol implemented by Telstra had prevented DDoS traffic on the Telstra link.

94. The traffic logs provided by Telstra and NextGen, as well as testing that had been carried out by IBM, enabled IBM to determine that the "hole" in Island Australia was a problem with the NextGen link and not the Telstra link.

95. NextGen had international links via two upstream suppliers, NTT and Vocus. At approximately 11.00 pm on 9 August 2016, Vocus joined a conference call between IBM, NextGen and Telstra. On that conference call, a Vocus representative [redacted] confirmed that there had been a "hole" in its implementation of the Island Australia

protocol. Vocus had failed to implement geo-blocking on one of its links through Singapore which had allowed further DDoS attacks to occur on the NextGen link.

96. Had Island Australia been properly implemented by Vocus the fourth DDoS attack would have been prevented, and the site would not have become unavailable to the public as a result.

97. There has been some speculation in the media[44] that the eCensus site did not have the capacity or was "not dimensioned properly" to handle the number of expected form submissions on 9 August 2016. That is simply incorrect. The ABS required IBM to design a system that could handle a peak rate of 250 form submissions per second. This is what IBM delivered. The system's capacity was comprehensively tested by Revolution IT as set out above. Immediately prior to the fourth DDoS attack, during the anticipated peak period for Census Night, the system was receiving in excess of 150 submissions per second – a submission rate comfortably within the system's capacity.

Period for which the eCensus site was unavailable

98. As noted above, under the terms of the 2016 Contract, the eCensus site was required to be available for 98% of the Main Event, which is the period from 9.00 am on 26 July 2016 to 12.00 midnight on 25 September 2016, a period of 61 days (1,479 hours), and for 98% of the Census Day Peak Period, being a period of 4 hours from 7.00 pm to 11.00 pm on 9 August 2016.

99. On 9 August 2016, the eCensus site was unavailable due to the fourth DDoS attack and IBM's decision to apply the overload control from approximately 7.27 pm to 10.29 pm, a period of approximately 3 hours out of the 4 hour peak period and 0.2% of the 1,479 hour Main Event period.

100. After 10.30 pm, the eCensus system was restored and in a stable, normal state. However, as explained above, at the direction of the ABS (and later the ASD), the overload control remained in place until 2.30 pm on 11 August 2016. The period that the eCensus site (and hence the electronic form) was unavailable to the public due to both the 7.27 pm DDoS attack and the decision to maintain the overload control in place was 43 hours and 3 minutes. That is, 2.9% of the 1,479 hour Main Event period.

101. IBM does not shy away from the fact that the period for which the eCensus system was unavailable was a critical period for the 2016 Census, nor does it seek to gainsay the inconvenience that has resulted from the system being disabled for that period of time. IBM notes, however, that seen from the perspective of the Main Event, when the end date of 25 September 2016 is reached, the eCensus site will have been available to the public, in the sense that electronic forms were able to be accessed, completed and submitted for 1,436 hours out of the 1,479 period stipulated in the 2016 Contract (as amended). The percentage availability will be 97.1%. The period for which the eCensus system will

[44] For example, article titled "Census 2016: ex-ABS chief blames managerial incompetence" authored by Sam Varghese (14 August 2016), article titled "Experts cast doubt on Census DDoS claims" authored by Daniel Palmer (19 August 2016) and article titled "Census 2016 Website Crash: DDoS Attack, Incompetence Or Something More Sinister" authored by Spandas Lui (10 August 2016).

have been in normal state and, subject to the direction of the ABS (and later the ASD), *able* to be made fully operational by removing the overload control will be 1,476 of the 1,479 hour period stipulated in the 2016 Contract (as amended). The percentage availability will be 99.8%.

No data egress from the eCensus site

102. The system developed by IBM for the 2016 eCensus employed a range of mechanisms designed to prevent data loss or compromise, including:

(a) use of separate DMZ and application zones, with no data kept in the DMZ (consistent with standard industry practice);

(b) the use of an Intrusion Prevention System and Site Protection server monitored by IBM's Security Operations Centre;

(c) encryption of all respondent data in transit (on all internal and external network links);

(d) encryption of all respondent data at rest (prior to entry into the database) using respondent specific encryption keys;

(e) separate data and administration networks for the servers;

(f) server configurations preventing login between internet facing servers; and

(g) dedicated environment and management infrastructure (servers and tools).

103. These mechanisms were subject to rigorous testing, as set out in paragraphs 55 to 59 above.

104. IBM has at all times treated the security of the data obtained from respondents to the 2016 eCensus to be the ABS' paramount objective. IBM was, and is, not in fact able to access the data obtained from respondents. It is only decrypted after it is handed over to the ABS, which has the unique decryption key.

105. There is every reason to conclude that the mechanisms developed by IBM to ensure the security of data obtained from respondents in the 2016 eCensus have been effective.

106. As noted above, during the fourth DDoS attack, IBM personnel identified an apparent "spike" in outbound traffic on the system's monitoring dashboard. Investigations were commenced immediately to confirm whether there was any possibility of loss or compromise of data from the system.

107. IBM's investigations confirmed that no loss or compromise of data had occurred. The "spike" in the outbound traffic was a false positive resulting from the effect of the DDoS attack on the system's monitoring devices, and that information was conveyed to the ABS and ASD during the early hours of 10 August 2016. IBM's investigations have revealed that the false positive reading occurred because the system was programmed to measure

and report the traffic volume of the eCensus site at 60 second intervals. Once the fourth DDoS attack was underway, the information was being reported for varying intervals but the dashboard was treating the information as though it had applied the standard 60 second interval. This resulted in an incorrect graphic creating the impression that there had been a spike of outbound traffic that could be data egress.

108. IBM understands that the ABS has also concluded that the security of the Census was not compromised and that no data was lost or compromised.[45]

109. Further, on 11 August 2016, the Australian Privacy Commissioner, Mr Timothy Pilgrim PSM, announced that, following regular contact with the ABS and a direct briefing from the ASD, he was satisfied that "personal information was not inappropriately accessed, lost or mishandled" and that the decision to shut down the Census website to "avoid any prospect" that the DDoS attack could include or otherwise facilitate a data breach was "a pro-privacy precaution".[46]

[45] ABS Public Statement, 10 August 2016, titled "ABS update – 2016 Census online form" and Public Statement, 11 August 2016, titled "2016 Census - Online form update".
[46] Australian Privacy Commission Public Statement, 11 August 2016, titled "Census 2016 Website Incident, August 9".