Chapter 6
The conduct of the 2016 census

6.1 The reference date for the 2016 census was 9 August. On this date, millions of Australian households paused to complete their census forms. Unfortunately, for many people, the evening was one of frustration as the website and phone systems put in place failed.

6.2 This chapter begins with a summary timeline of key events between 9 and 11 August 2016, before going on to discuss the failure of the eCensus website, problems with the telephone service, and the subsequent actions and conduct of census field officers.

Failure of the eCensus

6.3 This section provides a timeline of the events surrounding the failure of the eCensus website, and then considers the causes and response to this event.

9 August

6.4 During the morning of 9 August, the ABS experienced two Distributed Denial of Service (DDoS) attacks resulting in very short outages.[1] During the second attack the 'Island Australia' protocol—IBM's chosen DDoS defence—was enabled. This measure successfully stopped the attack and 'the ABS was of the understanding that the online form would now be protected from any further attacks'.[2] A third attack in the afternoon was repelled without any loss of service.

6.5 At approximately 7.00 pm, the eCensus website had already successfully processed over 1.8 million household forms and was running at 7 167 forms per minute, with demand growing in accordance with ABS modelling.[3] Commencing at 7.28 pm a fourth DDoS attack occurred resulting in the website being unavailable from 7.33 pm.[4]

6.6 At the time of the attack, the ABS and IBM observed a spike in outbound traffic in the IBM monitoring systems, prompting concerns that the system may have been compromised and experiencing data leakage.[5] IBM reported:

> [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

---

1 A more fulsome discussion of Island Australia and Distributed Denial of Service attacks are provided later in this chapter.

2 Australian Bureau of Statistics, *Submission 38*, p. 66.

3 Australian Bureau of Statistics, freedom of information disclosure, 25 October 2016, p. 50.

4 Australian Bureau of Statistics, *Submission 38*, p. 66.

5 Australian Bureau of Statistics, *Submission 38*, p. 66.

> 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.[6]

6.7 IBM attempted to reboot its system at 7.43 pm but was unable to restore services.[7] The committee heard that IBM had incorrectly configured at least one of the two routers it had in place.[8] When the routers were restarted the link to the Telstra network did not load its previous configuration; this left only the third party provider, Nextgen's link in place, and that link was consumed by DDoS traffic.[9]

6.8 At the request of the ABS, IBM enabled 'overload' controls at 8.09 pm which prevented Australian households from commencing new census forms.[10]

6.9 The Minister for Small Business, the Hon. Michael McCormack MP, was provided an initial briefing by the Australian Statistician at 8.26 pm.[11] At 8:38pm the ABS published a message through social media channels informing people that the census website was experiencing an outage, and at 8.50 pm, the ABS requested Dentsu Mitchell—a consultancy providing advertising for the census—cease all social and digital advertising.[12] The ABS was informed that advertising would cease by approximately 9. 40pm.[13]

6.10 IBM was able to successfully restore the online census system at 10.26 pm. At this point the ABS stated that it would have been possible to make the eCensus available to the public again. However, the ABS elected to keep the eCensus system closed until: it had understood the unanticipated spike in outbound traffic earlier in the evening; was sure it could defend against future DDoS attacks; and was sure that the infrastructure was robust including the routers which had experienced issues.[14]

6.11 At 10.59 pm, the ABS posted updates to social media stating that the eCensus service would be unavailable for the remainder of the evening, and that an update would be posted in the morning.

---

6 IBM Australia Limited, *Submission 87*, p. 3.

7 Australian Bureau of Statistics, *Submission 38*, p. 66.

8 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 48.

9 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard* , 25 October 2016, p. 16.

10 Australian Bureau of Statistics, Submission 38, p. 67.

11 Australian Bureau of Statistics, Submission 38, p. 67.

12 Australian Bureau of Statistics, *Submission 38*, p. 67.

13 Australian Bureau of Statistics, *Submission 38*, p. 68.

14 Australian Bureau of Statistics, *Submission 38*, p. 67.

10 August

6.12 It was reported to the committee that in the early hours of the morning, 'the ABS and IBM conclusively determined that both the outage was caused by an overseas-based DDoS attack and that no data was lost'.[15]

6.13 The ABS published a statement on 10 August explaining what had occurred the previous day:

> The 2016 online Census form was subject to four Denial of Service attacks yesterday of varying nature and severity.
>
> The first three caused minor disruption but more than 2 [million] forms were successfully submitted and safely stored.
>
> After the fourth attack, just after 7.30 pm, the ABS took the precaution of closing down the system to ensure the integrity of the data.[16]

11 August

6.14 On the morning of 11 August, the Australian Privacy Commissioner announced that he was 'satisfied that personal information was not inappropriately accessed, lost or mishandled'.[17]

6.15 At 1.16 pm, the Australian Signals Directorate (ASD) notified the ABS that IBM 'had taken all steps that could reasonably be taken in the time available to mitigate denial of service attacks similar to those that occurred on 9 August'.[18]

6.16 At 2.29 pm on 11 August, the system was reopened to the public.

What was the cause of the outage

6.17 The cause of the suspension of the eCensus website on 9 August was the ABS taking the *deliberate* decision to prevent households from logging onto the website. This decision was precipitated by a DDoS attack that was not adequately protected against, and was of such a small size that it should have easily been handled effectively. As explained by the Special Adviser to the Prime Minister on Cyber Security, Mr Alastair MacGibbon:

> There were indeed attacks, they should have been expected, they were expected, protection against them was contracted for—and these were definitely small attacks and they should not have degraded the ABS system. But it was not the denial-of-service attacks that actually eventually took the ABS e-census website offline. That was a decision made by the ABS, and there were two other critical components in there. The denial-of-service attacks that degraded the system, the attempts by IBM in turning the routers off to re-communicate with their data centre—finding that they had

15 Australian Bureau of Statistics, *Submission 38*, p. 68.

16 David W Kalisch, Australian Bureau of Statistics, 'ABS update – 2016 Census online form', *Media Release*, 10 August 2016.

17 Australian Bureau of Statistics, *Submission 38*, p. 69.

18 Australian Bureau of Statistics, *Submission 38*, p. 69.

> misconfigured the router at the Telstra end of the link—and then, in a sense, the final straw that broke the camel's back was the misinterpretation of data on a load-monitoring system, which was interpreted at first as possibly the exfiltration of data—or, an actual hack, as opposed to an attack.[19]

6.18 The influx of traffic to the IBM routers appear to have caused a malfunction within the internal monitoring of the IBM system:

> During the fourth attack, a system monitoring dashboard, which included a graph of inbound and outbound [Internet Service Provider] 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'.[20]

6.19 Due to fear that a recorded spike in outbound data traffic from the eCensus system represented a potential data leak, the ABS decided to temporarily close access to the website.[21]

What is a DDoS

6.20 IBM provided the committee with an explanation of how DDoS attacks operate:

> 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.
>
> 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.
>
> 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.
>
> 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.[22]

---

19 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 44.

20 IBM Australia Limited, *Submission 87*, p. 16.

21 Special Adviser to the Prime Minister on Cyber Security, *Submission 31*, p. 2.

22 IBM Australia Limited, *Submission 87*, p. 13.

6.21 DDoS attacks are neither new nor unusual. The committee heard that it is commonplace for government websites to regularly experience denial of service attacks which are routinely managed without interruption to services.[23]

6.22 It is unclear if the eCensus website experienced further DDoS attack attempts following restoration of the system. IBM informed the committee that there were further DDoS attacks which were successfully defended.[24] In contrast, the ABS claimed to be unaware of any further attacks.[25] The perpetrators of the DDoS attack remain unknown.[26]

What plans were put in place to prevent DDoS

6.23 The ABS was aware of the threats posed by a prospective DDoS and had contracted for measures to be put in place to mitigate them. The committee heard that DDoS events are routine occurrences, and are also routinely managed without incident:

> Denial-of-service attacks, or distributed denial of service attacks, are eminently predictable and should be expected. In fact, the Australian Bureau of Statistics did call for denial-of-service protection in its tender process with IBM, and IBM responded to say that they would put in place denial-of-service protection. So yes, it is expected, and it should be dealt with.
>
> …
>
> There were indeed attacks, they should have been expected, they were expected, protection against them was contracted for—and these were definitely small attacks and they should not have degraded the ABS system.[27]

6.24 The risks of DDoS attacks were included in the risk management plan for the 2016 census, with the ABS reporting:

> In the final risk management plan (July 2016), one of the risks was 'Loss of system availability through a Distributed Denial of Service Attack'. This risk had pre-mitigated exposure rating of 'high' and a residual exposure of 'medium'. Under the plan, IBM was responsible for mitigating this risk, with ISP measures of Island Australia (geoblocking international traffic) a key measure.[28]

---

23 Special Adviser to the Prime Minister on Cyber Security, *Submission 31*, p. 2.

24 IBM Australia Limited, *Submission 87*, p. 4; Mr Kerry Purcell, Managing Director, IBM Australia and New Zealand, *Committee Hansard* , 25 October 2016, p. 12.

25 Mr Jonathan Palmer, Deputy Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 32.

26 Special Adviser to the Prime Minister on Cyber Security, *Submission 31*, p. 2.

27 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 44.

28 Australian Bureau of Statistics, *Submission 38*, p. 62.

6.25 IBM states that it met its requirement to provide DDoS protection through the 'Island Australia' policy.[29] IBM explained how this mitigation strategy would work:

> 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.
>
> 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, legitimate traffic to the eCensus site could be expected to be domestic to Australia.[30]

6.26 IBM tested the Island Australia protocol on 5 August 2016 and reported to the ABS that it had 'worked exactly as expected'.[31] IBM reported that the success of this test gave them a high level of confidence that appropriate DDoS mitigation measures were in place:

> 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.[32]

6.27 While preparing for the eCensus, IBM 'considered other possible options for the defence of DDoS attacks'.[33] IBM examined other products offered for DDoS protection yet concluded that these services would not be suitable for the 2016 eCensus 'because of the unique traffic profile it was expected to generate'.[34]

6.28 In July 2016, the ABS and IBM received a briefing from ASD on cyber threats and incident response support. The ABS recalls:

> The potential for DDoS attacks was discussed, as were general mitigations for a range of threats. ABS does not believe that any new areas of concern were raised, nor were there any suggestions of potential mitigations or additional preparations that were not pursued.[35]

The failure of Island Australia

29 IBM Australia Limited, *Submission 87*, p. 2.

30 IBM Australia Limited, *Submission 87*, pp. 13–14.

31 Australian Bureau of Statistics, *Submission 38*, p. 62.

32 IBM Australia Limited, *Submission 87*, p. 15.

33 IBM Australia Limited, *Submission 87*, p. 15.

34 IBM Australia Limited, *Submission 87*, p. 15.

35 Australian Bureau of Statistics, *Submission 38*, p. 62.

6.29 IBM anticipated, and assured the ABS, that Island Australia would prevent international traffic from reaching the eCensus website, thereby ensuring that international traffic could not be used for a DDoS attack.

6.30 The internet is a network of networks, and in order to allow public access to a webpage, a company like IBM must pair with internet service providers (ISPs) to link the IBM network to the rest of the internet. Public access to the eCensus site was provided via two ISP links, one provided by Telstra Limited (Telstra) and the other by Nextgen Networks Pty Ltd (Nextgen).[36] If a serious DDoS attack occurred during the census collection period, IBM would direct Nextgen and Telstra to put in place Island Australia.[37] These ISPs would prevent the malicious traffic from reaching the IBM network processing the census data.

6.31 When a household attempted to fill in the eCensus the message needs to move from their home to the final destination; which in this case is IBM. In order for this to be possible, there needs to be a path along the networks of the internet from an origin and the destination. Suppose Alice wants to complete her eCensus. Alice's personal computer (A) would speak to her router (B), which would send a message to a router (C) operated by her internet service provider. That router (C) would try and pass the message to a router (D) owned by—in this case—either Telstra or Nextgen which have a direct link to the destination—IBM. If no such router can be found, it (C) would pass the message onto another network's router (E) which would attempt to pass the message onto a router (D) on the desired network. Once the message finds the correct network, the message will be delivered to IBM.

6.32 Under the Island Australia protocol, if any of the routers belonging to Telstra or Nextgen received a message that was addressed to the eCensus and sent from an international router (ISP), that message would not be processed.

6.33 Commencing at 7.28 pm, a DDoS attack began eroding the capacity of the system. The size of the attack was estimated to be around 1.5 gigabits per second.[38] The attack reportedly had the effect of commencing new sessions which quickly exhausted the memory capacity of the IBM's router facing the Nextgen link.[39] Mr MacGibbon noted that this attack was a '…weapon but a small one and one that we should have had protections against, absolutely' and '[it] certainly should not have caused the damage that it did'.[40]

6.34 IBM alleges in its submission that Nextgen failed to properly implement the Island Australia protocol which allowed traffic to flood the IBM system:

---

36 IBM Australia Limited, *Submission 87*, p. 14.

37 IBM Australia Limited, *Submission 87*, p. 2.

38 Australian Bureau of Statistics, answers to questions on notice, 21 September 2016, p. 6.

39 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard* , 25 October 2016, p. 23.

40 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 48.

> 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.[41]

6.35 IBM contends that had Nextgen properly implemented Island Australia the eCensus website may not have become unavailable:

> 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.[42]

6.36 Nextgen disputed this allegation, noting that they had implemented the same settings as IBM had successfully tested on 5 August 2016, and that their analysis demonstrated that both the Telstra and Nextgen links showed DDoS traffic during the fourth attack.[43]

6.37 Vocus Communications[44] (Vocus) informed the committee that it recorded a peak traffic load through the Singapore link of 563Mbps. Vocus' submission states that this 'is not considered significant in the industry' and 'not of a size to cause the census website to become unresponsive, had appropriate network security measures been implemented by IBM'.[45]

6.38 As previously discussed, IBM had two routers in place to facilitate Australians filling in their eCensus forms. Each router alone had sufficient capacity to transfer all of the anticipated legitimate census traffic. Representatives of the ABS, in a foray into biology, explained:

> At this point we knew we could operate with one router. We knew the system was designed to have sufficient capacity…I would say it is a bit like functioning on one kidney, but you do not really want to when you have two.[46]

6.39 Even though IBM reports that all of the DDoS traffic was coming through the Nextgen link, both routers appeared to be experiencing an unusually heavy load.

6.40 This heavy load adversely affected IBM's internal system monitoring the flows of data in and out of the network, eventually resulting in erroneous telemetry

---

41 IBM Australia Limited, *Submission 87*, p. 3.

42 IBM Australia Limited, *Submission 87*, p. 3.

43 Nextgen Networks, *Submission 88*, p. 1.

44 Following the 2016 Census, Vocus Communications acquired Nextgen.

45 Vocus Communications, *Submission 89*, p. [2].

46 Mr Jonathan Palmer, Deputy Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 33.

from automated monitoring systems that would lead to the eCensus website being disabled. As IBM explains:

> 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.[47]

6.41 This spike was what led IBM and the ABS to fear census data was being exfiltrated from the system. It has been suggested that the elevated data flow was IBM's computer system reporting performance information and logs to an offshore data centre.[48]

6.42 The DDoS attack had the effect of consuming the memory of the routers meaning they were unable to properly process requests. In order to restore the system to functionality, IBM reset the routers. When they did this, the router on the Telstra link did not restore its settings, meaning that the only link to the eCensus website was the Nextgen link which was subject to the DDoS attack.[49] Mr MacGibbon explained the problem on IBM's Telstra router:

> I think the biggest issue was that the router that was at the Telstra link was incorrectly coded by IBM, so when it was turned off the coding fell out, for want of a better description, from that router and it made it a 'dumb unit'. The time it then took to get it back up to scratch is where the confusion happened.[50]

6.43 IBM reports that it took one hour and twenty minutes to restore the Telstra link. Once the Telstra link was restored IBM reports closing the Nextgen link. IBM states that at this point there was an immediate drop in attack traffic and a resumption of normal application behaviour.[51] IBM reports that it was ready to restore the eCensus at 10.32 pm, approximately three hours after the site had become unresponsive.[52]

6.44 In summary, a DDoS attack adversely affected the operation of the routers' reporting system. When this reporting system displayed several minutes' of data at

---

47 IBM Australia Limited, *Submission 87*, pp. 19–20.

48 Dr Robert Merkel, *Submission 1*, p. 12.

49 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 17.

50 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 48.

51 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 17.

52 IBM Australia Limited, *Submission 87*, p. 4.

once—rather than the typical 60 second increment—it ignited fears that the system had been compromised. Further, IBM were unable to effectively reset their router to the Telstra network due to configuration errors. These two events, precipitated by the DDoS, led the ABS to take the decision to take the eCensus website offline. The combination of the three events ultimately led to the eCensus being unavailable. Mr MacGibbon observed:

> Anyone of those three things not existing—if there were no denial-of-service attacks or if they were properly mitigated—we would not have had the other two problems. If we had had the unmitigated denial-of-service attacks but the router had functioned properly, we would not have had the third problem, and we would not have had the third problem if the people that were monitoring the system properly interpreted the system, which was functioning oddly given the nature of the stresses that it was under, based on the first two points. So any one of those in isolation was not really sufficient to lead us to this committee today, some months later. It was the three combined that led us here.[53]

6.45 The natural question this raises is was the preparation and protection by IBM and ABS sufficient?

Were the protections put in place by IBM sufficient?

6.46 The events of the evening of 9 August would imply that mistakes were made in the preparation and execution of the DDoS defence. The IBM submission argues that Island Australia was approved by the ABS as a means of defending against DDoS attacks.[54] It appears that IBM and the ABS were in agreement that any botnet[55] in Australia was of insufficient size to cause serious damage to the eCensus website, and therefore geoblocking would be sufficient.[56]

6.47 However, Island Australia geoblocking was not the only option available to IBM in meeting its contractual obligations in ensuring resilience in the face of DDoS attacks. This report has already canvassed why Island Australia was thought by IBM to be sufficient.

6.48 It was put to the committee that Nextgen had raised concerns with IBM that the Internet Protocol (IP) ranges that IBM planned to block were not exhaustive, and that Island Australia may not adequately protect the eCensus.[57]

6.49 The committee heard that Nextgen offered IBM DDoS protection which was rejected by IBM.[58] IBM claimed that the Nextgen solution was not fit for purpose:

---

53 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 49.

54 IBM Australia Limited, *Submission 87*, p. 14.

55 A collection of network connected computers controlled from one or more central controllers. Botnets can be used to perform DDoS attacks by directing the individual bots to flood the desired websites with requests.

56 IBM Australia Limited, *Submission 87*, p. 14.

57 Nextgen Networks, *Submission 88*, p. 2.

> We looked at and considered the DDoS protection that was being offered by Nextgen and, on the basis of the information that they provided, there were three distinct attributes that we felt rendered it unsuitable. The first concern was that Nextgen advised us that it required a four-week training period to learn the particular traffic patterns that would be coming into the site. We did not have a four-week lead-in period during which to learn the traffic patterns. And the traffic pattern in the weeks leading up to census night is not at all representative of what we experience on the night.
>
> The second concern, which we discussed with Nextgen in advance of the RFT response being submitted in 2014, was the ability of their solution to deal with that very high peak we experience on census night and whether it in fact might be interpreted as a DDoS attack, and that they share that concern with us. The third was one related to the specifics of the application and the way we were doing load balancing to distribute the load across multiple back-end process streams. There was a concern early on in the process that the Nextgen protection approach might interfere with that load-balancing mechanism. So for those three reasons we felt that the geoblocking was a very well adapted solution for the particular characteristics of the traffic, and it is one which we had experience of in 2011, with both Telstra and Optus, that they could very effectively and easily implement, so we chose that as our preferred strategy.[59]

6.50 Evidence received by the committee indicates that the Nextgen solution was adopted after the resumption of the eCensus, casting doubt on explanations of why it would have been unsuitable before 9 August made by IBM.[60] IBM claims that the adoption of the Nextgen DDoS products following the resumption of the eCensus was in response to a changed threat environment where it had become public knowledge how the eCensus was being defended.[61]

6.51 The choice of geoblocking as the sole means of DDoS protection is interesting given a number of technical considerations related to the eCensus:

> There were some technical problems in that some Australians, with Australian-based ISPs, will also route in from overseas, just by the nature of the ways in which those ISPs operate. In fact, the password reset facility that IBM used actually relied on traffic coming in from overseas to give Australians that password. So there was a fundamental failure in the logic of an Island Australia. I could see it as part of a series of protections adding some value, but to rely solely on it clearly was a failure.[62]

---

58 Nextgen Networks, *Submission 88*, p. 1.

59 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 24.

60 Nextgen Networks, *Submission 88*, pp. 2–3.

61 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 24.

62 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 45.

6.52 Given that the eCensus system itself relied on communications from outside Australia, the proposal to protect the application by blocking this traffic appears curious.

6.53 It was pointed out to the committee that there was sufficient redundancy built into the system by having two ISP links. Had the Telstra router been properly configured such that when it was restarted it worked properly, the problems experienced on 9 August would likely have been avoided.[63]

6.54 IBM admitted that, in hindsight, further testing of the router would have uncovered the configuration error before it become an issue on census night:

> But we tested that router failure by simulating it, which is relatively easy to do in a repeatable fashion. If we had our time again, we would probably do a hard, powered-off powered-on test of that router. That would have discovered earlier that we had that reboot and configuration loading problem.[64]

6.55 There appeared to be some confusion on census night regarding what had actually happened with the router, with the ABS being initially under the impression that the router on IBM's Telstra link had suffered from a hardware failure.[65]

6.56 Mr MacGibbon highlighted that the greatest failure on the part of IBM was that they did not check that Island Australia had been properly implemented by its subcontractors.[66] IBM informed the committee that, with hindsight, they would have sought greater certainty that their geoblocking protocols had been correctly implemented by their contractors.[67]

6.57 IBM claims that they assumed that all of their contractors had the ability to implement their instructions:

> We as the prime contractor dealt with both Telstra and Nextgen as our ISPs and expected them, as large internet service providers, to be able to implement those instructions correctly.[68]

---

63 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 49.

64 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 19.

65 Mr Jonathan Palmer, Deputy Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 32.

66 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 45.

67 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 19.

68 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 19.

6.58 The committee is not in a position to determine the relative truth of where any fault lies between IBM and its contractors. Mr MacGibbon explained the situation between the parties nicely:

> The Commonwealth, in this instance, was the customer. The customer went to a builder to build a house. There were blueprints put before them as to what that house would look like, and the Commonwealth, as the customer, paid money to the builder to build the house. The builder is now in dispute with a plumber and a bricklayer about what was or was not done in relation to the deficient house. IBM, of course, being the builder and Vocus and Nextgen, when you look at their responses, being the plumber and the bricklayer…I cannot determine who is right and who is wrong. What I will say is that as the customer the Commonwealth was not well served.[69]

6.59 Extending on this example, the taxpayer has bought a house off the plan with a sinking foundation and cracks in the walls: they can feel rightly aggrieved.

Did the ABS have too much trust in IBM?

6.60 The ABS had contracted IBM to provide DDoS prevention measures, and IBM assured the ABS that this was done.[70] The ABS can rightly say that they expected the eCensus to be secure and stable in the face of threats:

> **Senator HUME:** Were you surprised by the extent of the disruption caused by the DDoS events considering on a relative basis they did not seem to be particularly large?
>
> **Mr Kalisch:** We were certainly surprised that the system was vulnerable.
>
> **Senator HUME:** And you were assured, I assume, beforehand; otherwise, you were assured that it was invulnerable?
>
> **Mr Kalisch:** We were assured that that system was robust and was ready to go to a range of different attacks and mechanisms, not just DDoS.[71]

6.61 It was suggested to the committee that the ABS showed too much trust in IBM and was not sufficiently proactive in ensuring that IBM was meeting their contractual obligations:

> In many respects, while I will say to you that this was a failure to deliver on the contractual obligations that IBM had, there was a failure on the part of the ABS to sufficiently check that the contract had been delivered. That could have been achieved through more thorough assessments of the work done for them by IBM and their subcontractors.[72]

---

69 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 47.

70 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 44.

71 Mr David Kalisch, Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 32.

72 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 45.

6.62 Mr MacGibbon suggested further that the ABS could have been more proactive in overseeing the implementation of the eCensus project to ensure that all contractual undertakings were being fulfilled:

> If I understand your question correctly, if they had engaged IBM, could they have verified that they were building the system that they were contracted to do? Yes, they could have. They could have had more third-party testing done. They may have asked more questions of IBM to provide proof that they were delivering the services they were contracted to do.[73]

6.63 The committee heard that the close relationship between the ABS and IBM could be interpreted as 'vendor lock-in', and that such relationships risk complacency in project management:

> **Mr MacGibbon:** …In relation to whether IBM was the natural choice—and I did hear the questions from the committee earlier—I do believe there was a degree of vendor lock in—that they were a trusted partner that had established a relationship over many years and were seen as the natural choice by the ABS to deliver upon the project. Whether that is right or wrong is really for others to decide. But certainly I came to the conclusion that there was a degree of vendor lock in there.
>
> **CHAIR:** There are risks associated with that type of closeness of relationship.
>
> **Mr MacGibbon:** I would not be here in front of you today if those risks were not real.[74]

6.64 This view is supported by the findings of the CapDA report—commissioned by the ABS to consider options in delivering the eCensus system—which reported that some prospective solution vendors believed that the ABS would not move away from IBM:

> Whilst the market scan revealed there are some potentially capable suppliers interested in bidding for this work and thereby generating competition, there were also substantial reservations expressed as to whether ABS would genuinely consider alternatives to IBM.[75]

6.65 One of the reasons cited by the ABS for partnering with IBM was their previous experience working with ABS systems and on the Censuses. As explained to the committee, the ABS assumed that IBM were familiar with their requirements:

> There was considerable clarity as to our requirements and their contractual obligations to meet those. We were building on our experience with two prior censuses, so they [IBM] had an excellent understanding of what we

---

73 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 46.

74 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 46.

75 Australian Bureau of Statistics, answers to questions on notice, 14 October 2016 (received 18 October 2016), p. 35.

> needed. So I do not think that there was any lack of understanding leading up to the census.[76]

6.66 This assumed familiarity may have contributed to a level of complacency in project management on the part of the ABS, and in the priority which IBM gave the project. The ABS could have been more proactive in ensuring DDoS protection was in place. Whereas the ABS contracted third parties to undertake load testing and code reviews, IBM was left to test their own DDoS prevention solution. It was suggested that an external party might have uncovered the hole in Island Australia that was not revealed through IBM's internal testing.[77] It has not been explained to the committee why IBM's testing showed Island Australia to be effective on 5 August, but was later to fail on 9 August.

6.67 The committee heard that the ABS did not undertake an Information Security Registered Assessors Program (IRAP) assessment. An IRAP assessment assesses the implementation, appropriateness and effectiveness of an information security system's security controls.[78] As explained by Alastair MacGibbon:

> The IRAP process is a process designed for third parties that are certified by or accredited by the ASD to come in and look at the architecture of systems—the schematics, for want of a better description—to ensure that they meet the information security requirements of the Commonwealth depending upon the level of security and protection needed in those systems. I would describe it as a compliance assurance process that should not be relied upon for all of IT security but is a practice that is necessary for ensuring that systems at least meet certain standards.[79]

6.68 The committee was further informed that it is not possible to know whether an IRAP assessment would have uncovered the flaws that allowed the DDoS attack to affect the eCensus.[80]

6.69 The relevant consideration here is whether the ABS should have had taken a more proactive oversight role in relation to the eCensus, and also whether they had the capacity to do so. CapDA's report that recommended the ABS partner with IBM was, in part, premised on the fact that ABS lacked the internal capacity to deliver the eCensus without outside assistance:

---

76 Mr Jonathan Palmer, Deputy Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 34.

77 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, pp. 45–6.

78 Department of Defence, *What is an IRAP Assessment?*, http://www.asd.gov.au/infosec/irap/irap_assessments.htm (accessed: 1 November 2016).

79 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 49.

80 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 49.

> CapDA's report, as you are aware, noted that we did not have sufficient in-house capacity to run that application ourselves and that we would need to look at procuring an external partner to host that application.[81]

6.70 CapDA's report highlights the professionalism and dedication of the staff at the ABS, but in the end recommends that the ABS did not have the internal capacity to develop and deploy an eCensus.[82] If they did not have the ability to develop a solution themselves, it stands to reason that they would only have a limited capacity to question and challenge a contractor employed to develop such a solution.

Why did it take so long for the eCensus to resume

6.71 The eCensus website was offline for over 40 hours; from around 8.00 pm on 9 August to approximately 2.30 pm on 11 August.[83] The committee heard that IBM was ready to resume collecting eCensus forms on the night of 9 August, but that the ABS wanted to ensure that the security of the eCensus application before proceeding further:

> As the protection of personal information was paramount for all concerned on census day, a cautious approach was taken by IBM, the ABS and ASD to ensure and verify that data security was never compromised before the site was restored. IBM was ready to restore the eCensus site after three hours, around 10.30 pm, but its closure was extended by 40 hours, following a direction given to IBM by the ABS.[84]

6.72 The committee heard that the ABS wanted to ensure that the eCensus website was no longer vulnerable to further DDoS attacks, that additional backups were in place, and that no data had been compromised before reopening the eCensus website. As the Australian Statistician explained:

> There were three particular aspects that we wanted to be satisfied about. One was about the security of the data which, as we say, was something that we were assured of after three am the next morning. The second aspect was really related to the nature of the router and that there was a working contingency, and that was something that was still the subject of some discussion on the following morning and through the following day. The third aspect was that—certainly against the backdrop of the system being vulnerable to a DDoS event on the night before—I wanted to be as sure as we could be that it would not be vulnerable to a second DDoS event. And so that was where there was further engagement with ASD—and Telstra

81 Mr Trevor Sutton, Deputy Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 35.

82 Australian Bureau of Statistics, answers to questions on notice, 14 October 2016 (received 18 October 2016), p. 7.

83 Australian Bureau of Statistics, *Submission 38*, pp. 67–9.

84 Mr Kerry Purcell, Managing Director, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 12.

> certainly assisted in that process as well—making sure that there were a number of additional protections put in place.[85]

6.73 Mr MacGibbon expressed his support for ABS' approach in delaying the resumption of the eCensus until satisfied that all faults had been rectified, observing:

> There would only be one thing worse than the site being taken down that evening after those four denial of service attacks, and then the confusion around the router and the outbound traffic, and that was to get the site back up and have it knocked back down again.[86]

6.74 Once the ABS was satisfied that the system was secure and robust, the Australian Statistician ordered that the eCensus website be reopened; the eCensus was back online at approximately 2.30 pm on 11 August.

Was any personal data at risk?

6.75 The eCensus website was shut down due to fears that personal information might be compromised. As discussed above, at around 7.30 pm there was an observed elevation of outgoing data from the eCensus website. Fears that this traffic representing personal data led to the website being shut down.

6.76 The system developed by IBM for the 2016 eCensus employed a range of measures to prevent any loss of data.[87] IBM explained to the committee that:

> In terms of the primary security objective here of protecting respondent data, we had encryption mechanisms in place to ensure that the data was fully encrypted while it was in transit—in flight from the respondent to the census site—and that it was encrypted while at rest and stored within the backend of databases. IBM does not have the keys to be able to decrypt that data, so we have not and have never been at any point able to see any of the respondent data that is stored on our systems. So encryption is the primary mechanism that ensures the integrity and protection of the data from external inspection.[88]

6.77 These keys are in the possession of the ABS and are necessary to extract any meaningful data from the census forms.[89]

6.78 The ABS reported to the committee that they were confident that eCensus data had been secure at all times:

> I have to say I was confident all along that there was no breach, because of the nature of the security architecture. We had end-to-end encryption; we

85 Mr David Kalisch, Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 31.

86 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 47.

87 IBM Australia Limited, *Submission 87*, p. 19.

88 Mr Michael Shallcross, Distinguished Engineer for Global Technology Services, IBM Australia and New Zealand, *Committee Hansard*, 25 October 2016, p. 21.

89 IBM Australia Limited, *Submission 87*, p. 19.

> had had the architecture well reviewed. So the problem was that we could not explain this—as it turned out—false positive alert, and IBM could not explain to us what it was. We felt it was extremely important that we be able to assure the Australian public that our faith in our security was well placed.[90]

6.79 The Australian Privacy Commissioner and Acting Australian Information Commissioner 'received the necessary assurances [he] required to be satisfied that the personal information being collected as part of the 2016 census was secure'.[91] The Special Advisor to the Prime Minister on Cyber Security was also clear that no data was at risk:

> There has been no dispute with any party that no data was lost from the census, and there is agreement that there was encryption from end to end and that the ABS held the keys to decrypt.[92]

6.80 Evidence to this inquiry from parties involved with either the events or the investigation on 9 August 2016 are all in agreement that no personal data was incorrectly accessed or released.[93]

Committee View

6.81 It goes without saying that the eCensus website should have had the capacity to withstand what was a relatively minor attack. IBM designed the system so that even if one link was disabled, the second should have been sufficient to carry legitimate traffic and continue processing census forms.

6.82 Criticisms made with the benefit of hindsight must necessarily be tempered, but there appears to have been significant and obvious oversights in the preparation of the eCensus. IBM's failure to have tested a router restart, or have a backup synchronised and in place, appears to have been significant contributing factors to the failure of the eCensus on 9 August. Further, the appropriateness of Island Australia must also be questioned given that some components of the eCensus—such as password resets—required access to international servers. Although it is impossible to say with certainty and hindsight what would have been had the ABS made different decisions, allowing IBM to undertake their own testing and the failure to complete an IRAP assessment appear to be significant oversights in project management.

6.83 The ABS' primary consideration during the period under discussion was to complete an accurate census of Australia. As discussed in preceding chapters, community trust is a central ingredient of a reliable census, and the ABS has

---

90 Mr Jonathan Palmer, Deputy Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 31.

91 Office of the Australian Information Commissioner, *Submission 68*, p. 1.

92 Mr Alastair MacGibbon, Special Advisor to the Prime Minister on Cyber Security, Department of Prime Minister and Cabinet, *Committee Hansard*, 25 October 2016, p. 45.

93 Mr Kerry Purcell, Managing Director, IBM Australia and New Zealand, *Committee Hansard* , 25 October 2016, pp. 12, 19; IBM Australia Limited, *Submission 87*, p. 2; Special Adviser to the Prime Minister on Cyber Security, *Submission 31*, p. 2.

repeatedly said that information security is one of its primary objectives. In light of this—and the information available to the ABS through the IBM monitoring system—the decision taken by the ABS on the evening of 9 August to close access to the eCensus website appears to be justifiable, understandable, and entirely correct.

6.84 A narrow focus on the events of August risks treating the symptoms and ignoring the disease. Questions regarding the validity of the ABS' actions should be focused on the years and months before the 2016 census when the decisions were made that would manifest themselves on 9 August 2016. The confirmation that the census would proceed, the delayed development of an eCensus solution, the use of a limited tender and the erosion of internal capacity to adequately oversee the development of the eCensus are all serious concerns that may contributed to the events of 9 August 2016.

6.85 The committee expected that the 2016 census would be subject to the two-pass ICT Investment Approval Process (IIAP) outlined by the Department of Finance.[94] The census project had lifetime ICT costs over $10 million once IBM, UXC Saltbush and Revolution IT contracts were taken into account. Further, as recognised by the ABS, the 2016 census was a high risk project.[95]

6.86 The ABS told the committee that the Department of Finance determined in October 2012 that the 2016 census was not required to complete to the IIAP.[96] In answers to questions on notice, the Department of Finance noted that the project did not meet the criteria for inclusion in the IIAP.[97] The committee notes that the ICT Review document recommending tendering for the eCensus was not completed until May 2014. The committee considers that the IIAP is in need of review to ensure that:

(a) projects such as the 2016 census fall within scope;

(b) the Department of Finance re-assesses projects at a later date if required; and

(c) the splitting of contracts is not a mechanism to skirt whole of life cost limits included in the IIAP.

6.87 The committee makes no suggestion that the Department of Finance acted inappropriately or that the ABS split contracts to minimise value-based scrutiny.

6.88 The committee also notes that the responsible Minister has not taken responsibility for the outcomes of the 2016 census. The committee calls on the current

94 Department of Finance, 'ICT Investment Approval Process', https://www.finance.gov.au/policy-guides-procurement/ict-investment-framework/ict-two-pass-review/ (accessed 21 November 2016).

95 Mr David Kalisch, Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, pp. 37-38.

96 Mr Trevor Sutton, Deputy Australian Statistician, Australian Bureau of Statistics, *Committee Hansard*, 25 October 2016, p. 38.

97 Department of Finance, answers to questions on notice, 18 October 2016 (received 18 November 2016), p. 2.

Minister, on behalf of the government, to take responsibility for the shortfalls in oversight that have been revealed through this inquiry. While many parties have not lived up to their responsibilities in delivering the 2016 census, the primary responsibility lies with the government.

Recommendation 4

6.89 The committee recommends that the Australian Government commit the necessary funding for the 2021 census in the 2017–18 Budget.

Recommendation 5

6.90 The committee recommends that the ABS conduct open tendering processes for future census solutions requiring the participation of the private sector.

Recommendation 6

6.91 The committee recommends that the ABS give greater attention to intellectual property provisions in contracts that include licensing and royalty arrangements.

Recommendation 7

6.92 The committee recommends that the 2021 eCensus application be subject to an Information Security Registered Assessors Program Assessment.

Recommendation 8

6.93 The committee recommends that the ABS take a more proactive role in validating the resilience of the eCensus application for the 2021 census.

Recommendation 9

6.94 The committee recommends that the Department of Finance review its ICT Investment Approval Process to ensure that projects such as the 2016 Census are covered by the cabinet two-pass process.

Recommendation 10

6.95 The committee recommends that the Australian Government provide portfolio stability for the ABS.

Recommendation 11

6.96 The committee recommends responsible ministers seek six-monthly briefings on the progress of census preparations. These briefings should cover issues including, but not limited to, cyber security, system redundancy, procurement processes and the capacity of the ABS to manage risks associated with the census.

Census Inquiry Service

6.97 In addition to the eCensus website suffering a prolonged outage, the telephone-based Census Inquiry Service (CIS) also buckled, but this time under the demands of the community. As the ABS explained:

> Due to a range of factors including public concerns regarding fines that had been unprompted by the ABS, faster than expected postage of approach letters and a general high awareness of the Census, the CIS experienced unprecedented demand that greatly exceeded ABS forecasts. The unavailability of the online Census on Census night significantly exacerbated the number of calls. This led to significant 'call blocking' and inconvenience for Australians both in the lead-up to and on Census night. We apologise for this, and the ABS will take account of this experience in planning future Censuses.[98]

6.98 The ABS reported that the demand forecast for the 2016 census was 1.6 million calls, compared with 1.04 million calls received for the 2011 census.[99] The committee heard that by 8 September 2016 there had been 3.2 million attempts to call the CIS, of which 1.1 million had been answered. In addition there were 1.6 million calls to the automated inquiry service, of which 0.9 million were handled electronically.[100]

6.99 The ABS outlined their strategy for dealing with excess demand should it eventuate:

> It was decided that the strategy for managing excess calls would be to politely request that callers call back later if the queues are at capacity, rather than provide callers with long wait times. This strategy is known as call blocking.[101]

6.100 The ABS submission concludes: 'The use of call blocking meant that 90.8 [per cent] of callers that got through to the CIS had their calls answered within 5 minutes'.[102] For the approximately one-in-three people who managed to make it onto the phone queue, the wait was relatively short.

6.101 Some submissions reported that people were unable to request a paper form in a timely manner due to excess demand on the CIS, meaning that their paper forms arrived well after 9 August.[103] Other submitters reported that their request for paper forms was not processed correctly or in a timely manner.[104] It was pointed out to the committee that households that do not have a telephone or internet connection would not have had any way to complete their census or obtain a paper form in 2016: a challenge that was previously circumvented by the physical delivery of paper forms to

98 Australian Bureau of Statistics, *Submission 38*, p. 4.

99 Australian Bureau of Statistics, *Submission 38*, p. 65.

100 Australian Bureau of Statistics, *Submission 38*, p. 65.

101 Australian Bureau of Statistics, *Submission 38*, p. 65.

102 Australian Bureau of Statistics, *Submission 38*, p. 65.

103 Dr Cassandra Cross, *Submission 66*, p.2; Name withheld, *Submission 61*, p. [1].

104 Mr John Denman, *Submission 23*, p. [1].

every household.[105] These households were likely followed up by Field Officers at a later date.

6.102 The problems affecting the telephone service were of particular concern to vision impaired Australians who were required to contact the telephone system in order to access the 12-digit code for the census, clarify information about the accessibility of the online forms, or request the census in an alternate form.[106] The Science Party also expressed concern that the unavailability of both the eCensus and CIS may adversely affect the response rate to the census.[107]

6.103 It was put to the committee that having to request a paper form via a telephone service added an additional unnecessary step that households had to complete in order to undertake the census.[108] ID Consulting, an Australian based demographic consultancy, argued that:

> There is a large segment of Australia's population who would prefer a paper Census form (particularly older residents), but the phone lines were jammed and these households were unable to get through. In any case asking a household to ring up to enable them to respond to the Census in their preferred way creates another level of impediment to responding and reduces the response rate.[109]

6.104 The committee heard that community perceptions that the census had to be completed on the night of 9 August or face a fine added to general frustration and distress.[110] Vision Australia, for example, told the committee:

> Vision Australia spoke to people who were deeply distressed by the lack of information available; their anxiety was exacerbated by the threat of fines for not completing the Census on time. The abrupt message left on the service that people should call back later only added to this confusion.[111]

6.105 Vision Australia recommended that future Censuses should feature a dedicated, separate telephone service for people who require alternate formats or assistance to complete the census.[112]

---

105 Dr David Lucas, *Submission 33*, p. 1.

106 Vision Australia, *Submission 76*, p. 3.

107 Science Party, *Submission 56*, p. 3.

108 Dr David Lucas, *Submission 33*, p. 1; Executive Council of Australian Jewry, *Submission 26*, p. 3.

109 ID Consulting Pty Ltd, *Submission 39*, p. [3].

110 ID Consulting Pty Ltd, *Submission 39*, p. [6].

111 Vision Australia, *Submission 76*, p. 3.

112 Vision Australia, *Submission 76*, p. 4.

Recommendation 12

6.106 The committee recommends that the ABS consider establishing a dedicated telephone assistance line for people who require special assistance in completing the census.

Development, delivery and collection of census forms and materials

6.107 In June 2014, the ABS signed a Memorandum of Understanding with Australia Post to support the 2016 census.[113] The ABS explained that Australia Post's mail service was used to deliver and return required materials from the majority of households.[114] Households that were going to respond online received a log-in code via the post, and households that requested a paper census form would have delivered and returned that information via the post.

6.108 In preparing for the 2016 census, the ABS attempted to anticipate local needs by tailoring delivery to area needs:

> In some areas of Australia, where the postal service was likely to be unsuitable or insufficient address information was known, Census Field Officers delivered materials to each dwelling, enabling residents to either complete their form online or mail back a paper form. In other areas where a high proportion of residents were expected to need to complete the Census form on paper, all households were delivered paper forms in addition to login numbers.[115]

6.109 Despite the relative surety of the mail system in Australia, some submissions claimed that residents at certain addresses were not provided with census information. One such example related to the committee states:

> We know of one elderly person in our community, whose address was apparently not listed by the ABS, who did not receive the letter at all, and had to go to extraordinary lengths to obtain the census questionnaire form. The person has lived at that address for 48 years and reports having had no difficulties in receiving previous census forms and completing them.[116]

6.110 It was put to the committee that the correspondence from the ABS with the log-in codes for the eCensus had the appearance of junk-mail and may have been discarded by some residents.[117] From the perspective it of survey design, ID Consulting observed:

---

113 Australian Bureau of Statistics, *Submission 38*, p. 51.

114 Australian Bureau of Statistics, *Submission 38*, p. 53.

115 Australian Bureau of Statistics, *Submission 38*, p. 53.

116 Executive Council of Australian Jewry, *Submission 26*, p. 3.

117 Australian Population Association, *Submission 54*, p. [3]; Executive Council of Australian Jewry, *Submission 26*, p. 3; Ms Rosie Williams, *Submission 85*, p. [51].

> Lack of personal contact with a collector on delivery means households are less engaged with the Census and the mail-out logins were often ignored or thrown in the bin as junk mail.[118]

6.111 The ABS submission highlights the lengths they went to in order to support the community to complete their census forms:

> In partnership with CSIRO, ABS developed and tested the Census instruction letter, reminder letter and their envelopes to best support the Australian public undertaking the required actions – completing the Census online or requesting a paper form. Forty-nine variants were tested through random control trials, in order to select the best approach letters to households and reminder letters where completed forms had not been submitted.[119]

The role of field officers

6.112 One of the largest logistical elements of the census is recruiting the large number of Census Field Officers (CFOs) required to assist households complete the census. Approximately 38 000 temporary staff were recruited for the 2016 census.[120]

6.113 The evidence received by the committee amply highlighted some of the challenges in conducting such a large project that incorporates new elements such as the eCensus and form mail-outs. Some submitters felt that the conduct of CFOs was inappropriately persistent and aggressive. It was reported by one CFO that:

> Field Officers were required to adhere to a strict timeline for visiting dwellings, with five visits scheduled over three weeks from 26 August to 16 September. Given the context of 'I've got until 23 September', this was seen as tantamount to harassment by many householders, who resisted what they perceived as unreasonable pressure to comply.[121]

6.114 At least one CFO reported to the committee cases where the households were visited multiple times because of insufficient information sharing.[122]

6.115 Others felt that the ABS—as represented by CFOs—were insufficiently proactive in following up on households.[123] The committee was told that CFOs in many mail-out areas did not commence their visits until two weeks after census night, by which time the census was no longer 'front of mind' for many people.[124] This appears to be a consequence of the move to a digital first census which reduced the role for CFO:

---

118 ID Consulting Pty Ltd, *Submission 39*, p. [2].

119 Australian Bureau of Statistics, *Submission 38*, p. 55.

120 Australian Bureau of Statistics, *Submission 38*, p. 55.

121 Name withheld, *Submission 59*, p. 4.

122 Name withheld, *Submission 90*, pp. 3–4.

123 ID Consulting Pty Ltd, *Submission 39*, p. [3].

124 Name withheld, *Submission 59*, p. 4.

> The use and approach of reminder letters were planned to allow half of all Australians to respond to the Census before household visits were required. Household visits were planned to provide support to any households that required it, deliver additional materials and remind households to complete the Census.[125]

6.116 Additional concerns raised in submissions included issues such as insufficient training, an over-reliance on CFOs using personal resources to ensure the success of the census, and that the information flows between the ABS and CFOs were insufficient.[126] As the face of the census in the community, CFOs were the ones who were left to motivate people to participate in the census following the events of 9 August.[127]

125 Australian Bureau of Statistics, *Submission 38*, p. 53.

126 ID Consulting Pty Ltd, *Submission 39*, p. [5]; Name withheld, *Submission 90*, pp. 3–8.

127 Name withheld, *Submission 59*, p. 3.