Review of the Events Surrounding the 2016 eCensus

Improving institutional cyber security culture and practices across the Australian government.

13 October 2016

Alastair MacGibbon

Special Adviser to the Prime Minister on Cyber Security

EXECUTIVE SUMMARY

The Australian Government's new paradigm of online engagement and services for Australians is not coming. It's already here.

Government's response to the eCensus events of 9 August 2016 provides an opportunity to change the conversation about cyber security: to one of trust and confidence in the government's digital transformation agenda, where 'digital first' is the overwhelming preference for Australians, underpinned by tangible security and adherence to privacy.

The 2016 eCensus tells us that more of the same is not enough: there is a new imperative to embrace cyber security as a core platform for digital transformation. And when we make the necessary changes we will increase the chance to deliver on the promise of Australia's Cyber Security Strategy, to strengthen trust online and better realise Australia's digital potential.

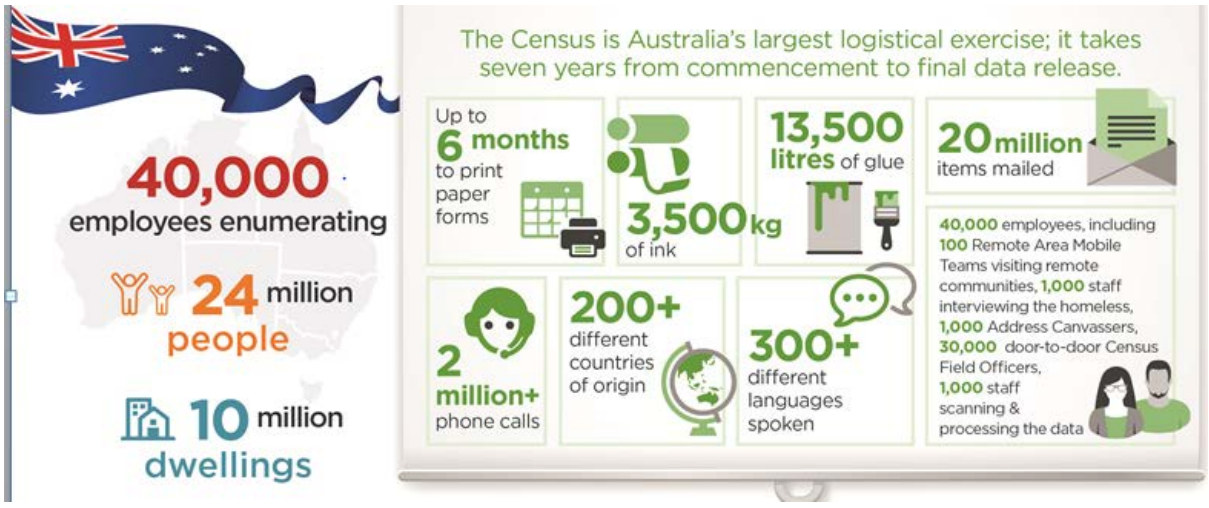
Much of the Government's dealings with Australians now takes place online, and this trend will only accelerate. But because this world is new, some disruption is bound to occur as culture shifts. And setbacks are inevitable.

The 2016 eCensus was a setback. One of the government's most respected agencies – the Australian Bureau of Statistics (the ABS) – working in collaboration with one of the technical world's most experienced companies – IBM – couldn't handle a predictable problem.

As a result, a key national event trended online globally as #CensusFail – a serious blow to public confidence in the Government's ability to deliver on public expectations.

While the media proclaimed the usual "cyber attack", this cyber security issue was, unusually, not a matter of national security. Instead, it was a clear demonstration of the broader impacts – and relevance – of cyber security on Australian society.

"Australia's largest peacetime logistical operation"



The ABS often cites “Australia’s largest peacetime logistical operation” and its proud history of 100 years of conducting censuses for Australians. The scale of the Census is immense and it touches the lives of all Australians. And in 2016 it worked hard to get more Australians to participate online. But this part of the Census represented significant risk.

In perspective, at around $9.6m – a fraction of the $471m overall spend on the Census – the payment to IBM to deliver the eCensus capability was small. Certainly the sum was small to IBM: between 1 January 2013 and 19 August 2016 IBM was awarded 777 contracts across the Commonwealth Government with a total value of $1.55 billion ($13.7m of which was with the ABS).

But cost isn’t the only issue. Nor the most important one. Australia now knows that cyber security is not just about national security. Cyber security is about availability of services and confidence in government in a digital age. And the public’s confidence in the ability of government to deliver took a serious blow, more so than any previous IT failure.

Even though the denial of service attacks on the night were predictable and defeatable, the decision to close off the eCensus was justified and no data were lost. The outcome could have been worse. But crucially important is the need to understand how the Census got to the point where the cyber security arrangements brought into question the trust and confidence in a fundamental government service. The public’s lack of confidence will linger. The integrity of the collection and its data are of critical value to Australia.

Looking at the issue and its impact through the cyber security lens, lessons are clear: about managing risk, about security in a digital age and about Australia’s digital future.

Crisis communications and coordination

The nature of the eCensus event, its national implications and the breadth of consequences of something going wrong were clearly underestimated in crisis planning. While the ABS and IBM had a library of incident management documents to guide them through the events of 9 August, they were impractical, poorly tested and none outlined a comprehensive cyber incident response or communications plan that could be effectively implemented.

Further, whole of government cyber security incident management arrangements did not link the affected agency with support mechanisms, leading to sub-optimal communication with Ministers and the public. Escalation thresholds were not clear, nor were obligations and coordination mechanisms across agencies.

The impacts of cyber security events are not well understood. There is not a shared understanding across government, and a well-defined lexicon does not exist. A whole of government approach to resilience is required, and regular exercising of crisis arrangements will be critical.

Security is a risky business…

The ABS’s problems on the night of 9 August stem from decisions taken well before then: decisions about partnership, procurement and project governance. Organisational culture and skills also played a part.

Security architecture

No system connected to the Internet can have guaranteed security. But as more government services move online, project managers will need to address security and respond to security incidents as critical business risks.

The distributed denial of service (DDoS) protections for the eCensus were inadequate, yet were called for in the ABS sole-sourced request for tender (RFT) and written into the contract with IBM. DDoS was a foreseeable threat, and more robust security planning would have led to a different outcome. Controls were not considered within a comprehensive security framework; risk assessments underestimated the consequences of security incidents, leading to insufficient focus on mitigations; and there was poor independent assessment or verification of security arrangements.

ABS and IBM emphasised some areas of security – the confidentiality and integrity of data – while underinvesting in the availability of the system.

The exchanges between the ABS, the Australian Signals Directorate (ASD) and IBM also suggest a lack of clarity in capacity, roles and responsibility for cyber security across government and with contracted service providers. Agencies look to ASD for advice to provide assurance; this may lead to a false sense of confidence. ASD endeavour to provide comprehensive advice and assistance. However, ASD's ability to provide an integrated assessment will be limited by their available resources and the time available to address the request. ASD have outstanding expertise for supporting agencies, but not the capacity to service the clear need across government. A new approach is needed for agencies to meet Australians' expectations of a modern digital government.

Protecting Australians' privacy

The DDoS attack against the eCensus system did not include the compromise of personal information of Australians. In fact, the ABS's decision to shut the eCensus website on 9 August was a privacy-protective measure.

However, the closure of the website appears to have amplified existing community concerns about security and privacy in relation to the Census; concerns which originated from an ABS decision to retain names and addresses for up to four years in Census 2016, in combination with the move to 'digital first'. There is more that the ABS can do to improve its practices, from external scrutiny to enhanced public engagement on privacy issues. All agencies can learn from the ABS's experience.

Not just communications, but engagement…

In most respects, the ABS had a well formed and prepared communications strategy and awareness raising campaign; but it was focussed on the wrong things. The communications problem they needed to address was not a low level of awareness of the Census, but rather, the introduction of a 'digital first' approach and the associated barriers to participation – concerns over security and privacy.

The ABS failed to adapt its media and communications in response to the public relations storm that built up in the weeks prior to the Census regarding privacy and security in both mainstream and social media. Instead, ABS rigidly stuck to its plans, forgoing crucial opportunities to influence and

drive the conversation around the Census. Processes for approval of campaigns, and changes to them, may need to be changed to promote agility.

On Census night, the ABS severely underutilised social media as a communications tool to keep the public up to date and informed of the incident. The ABS's lack of timely and transparent communications lost it trust because it opened the door to speculation. The continued slow updates and virtual absence from the media meant that ABS struggled to win back the trust of the public in the following days. Ministers must also be supported with clear and accurate advice, and senior executives must be equipped to understand and talk about cyber security as a matter of business risk.

Procurement, contracting and governance

Procurement practices fell short. Vendor lock-in, coupled with a particularly close and trusting relationship between the ABS and its long-term supplier IBM, meant that the ABS did not seek sufficient independent verification and oversight of critical aspects of the eCensus. Documentation suggests that there was compliance – risk matrices completed, committee meetings held, minutes taken – but the security culture was not resilient and adaptable. The ABS and IBM had delivered eCensus services for the 2006 and 2011 Censuses as well, the latter with a third of the population utilising the online form. Why should 2016 be any different?

The risk appetite of the ABS was not clearly defined: harm and consequence assessment appeared underestimated – particularly associated with security risks to the eCensus – leading to unsatisfactory risk mitigation strategies.

A lesson in culture

Culture matters. And the culture of the ABS identified by the Australian Public Service Commission (APSC) Capability Review in 2013 — insular, inward looking, reactive — affected decisions and performance as the ABS planned and carried out the 2016 Census. Moreover, its reliance on past patterns to guide future strategies doesn't work.

The prevailing culture can be identified in actions and decisions taken to prepare for the 2016 Census that date back to June 2012. Many seem innocuous, and almost all are compliant with established government practice. In many ways, the ABS is seen as an exemplar of established government practice: ticking the boxes, but not appreciating the challenges change presents.

There is no doubt that the preparations for the 2016 Census occurred during a complex time for the ABS. They were without a substantive Australian Statistician for most of 2014. However, it is clear that the ABS's culture clearly contributed to the outcomes on Census Night. The ABS's actions since only underscores the importance of culture: it has steadfastly refused to own the issue and acknowledge responsibility for the factors leading to the events and shortcomings in the handling of events on the night.

Over the last few years the ABS has devoted energy and resources to aggressively address the cultural issues highlighted in the APSC Capability Review. The ABS must draw upon the lessons it takes from the Census experience to help guide and advocate the cultural change path it is following.

Integrity of the Census

The Census outages prevented Australians from filling in forms online for almost 43 hours. This not only precluded online responses during the outages, but also likely reduced online responses over subsequent days due to confusion about security and the status of the eCensus. Considerable catch up then followed and many more Australians than planned turned to paper forms.

58 per cent of households participated online, up from 33 per cent for the 2011 Census. But ahead of the Census, the ABS had expected that 65 per cent of households would participate online. 2016 online return rates did not reach what were expected or desired.

Short delays in response do not impact on data quality. Many more households than usual not completing the Census by the end of the data-collection period would reduce quality.

The Census response rate, a critical indicator of quality, is estimated to be over 96 per cent. At this stage, it is unclear if the target rate of 96.5 per cent will be met. This target is based on the rate achieved in the 2011 Census.

A more granular assessment of Census quality will not be available until data has been processed, which will be completed by March 2017. Other indicators of data quality, such as refusals and item non-response rates, are likely to be comparable to, or better than, outcomes in the 2011 Census.

Unaware of these encouraging signs, post-Census surveys of public attitudes towards the 2016 Census find that many Australians believe that the data collected is unreliable. The latest Survey found that:

- **42 per cent agreed, to some extent, that this year's Census has been a failure; and**
- **33 per cent agreed, to some extent, that the data collected from this year's Census are unreliable.**

For the Census to be fit-for-purpose, the users of the statistics, and the public more generally, need to see the Census as credible. This credibility is to ensure that Census statistics are used for their intended purpose and that the public continues to provide quality responses to future Censuses.

Cyber Security for Australia's Digital Future

The ABS's experience provides insight into agencies' ability to operate in a digital age. Unpacking the incident, the scope is broad-ranging: issues facing the ABS included dealing with privacy issues in a dynamic technology environment, while adapting communications to new forms of online media.

The ABS did not look at alternate service options, such as cloud service provision. Cloud computing can offer significant security, cost and efficiency benefits, but the ABS's interpretation of privacy obligations of the Census and Statistics Act, and a lack of maturity in cloud service offerings at the time the contract was established, impeded take-up of cloud services which were limited to serving static content. There are likely similar barriers to cloud take up across government.

Digital awareness, including security risks and consequences, needs to be a core part of toolkits to deliver services in a modern online economy, where the needs and expectations of the community rapidly evolve. Small agencies such as the ABS are probably ill-equipped to deliver technology outcomes of scale.

The August 2015 review on 'Learning from Failure', by Professor Peter Shergold AC, called for more adaptive government and enhanced responsibility and accountability for program management. There are opportunities to adopt learnings from the eCensus incident in Phase Two of the government's Digital Transformation Agenda: security must be 'baked in' to design and delivery. Government can develop a more 'shared service' consultancy approach to cyber security to boost agency capacity.

So what now…

The ABS is likely not alone. Agencies need to transform their thinking to support a truly digital engagement with Australians. And cyber security and privacy was shown to be critical to the confidence of Australians in the online services delivered by government, and therefore in government itself.

While the eCensus delivery was a single technical project, it was also a step toward the government's future digital services agenda. And the setback the Census suffered must lead to a significant mindset shift that all agencies will need to make: digital disruption of their own service delivery.

All agencies must learn from the ABS's experience. This report contains:

- actions to improve the fundamentals supporting the transformation to secure online-government;
- improvements to the ABS approach to technology risk, procurement and governance;
- better practice recommendations for agencies as they make the transformation to online government.

Summary of Recommendations

- **Crisis Communications and Coordination:** The Department of the Prime Minister and Cabinet should strengthen cyber security incident management arrangements across government and ensure the policy is widely circulated, well understood and regularly exercised. This includes:
    - incorporating lessons learned from the eCensus incident response into the Cyber Incident Management Arrangements (CIMA);
    - ensuring effective crisis incident notification and coordination arrangements across Australian Cyber Security Centre agencies and between the Australian Cyber Security Centre, the Crisis Coordination Centre and the Department of the Prime Minister and Cabinet;
    - developing communications strategies, with key talking points for a range of cyber security incident scenarios; and
    - developing a whole-of-government 'cyber security lexicon' to assist with clear and consistent communication relating to cyber security issues.
- **Education:** The Attorney-General's Department should develop a "Cyber Bootcamp" for senior government executives and Ministers as part of the Cyber Security Strategy Awareness program. The Bootcamp would educate participants about cyber security fundamentals and how to talk about issues with the public and be aligned to Data61's work with the Australian Institute of Company Directors.
- **Security Framework:** The Australian Signals Directorate should strengthen the framework to help agencies improve the security of their networks:
    - update the Information Security Manual about security measures to protect the availability of online services;
    - in collaboration with the Digital Transformation Agency, lead a 'sprint' to lift agency capabilities to protect against denial of service attacks; this should provide a pilot model for future 'sprints' to build cyber security capacity across the Commonwealth;
    - develop and implement a security framework for high-risk online essential services and special events, to complement the high risk agency security framework identified in the Cyber Security Strategy; and
    - review its model for prioritisation and proactive engagement with agencies to provide cyber security support and develop a service catalogue of offerings to ensure clear understanding of capabilities; this may require additional resources to achieve. The Australian Signals Directorate should come back to government with a plan coordinated with the Cyber Security Special Adviser.
- **Creating a Positive Risk Culture:** The Department of Finance should assist agencies to actively engage with cyber security risk by developing:
    - guidance for managing risk in ICT and cyber security outsourcing; and
    - a strategy to accelerate government to improve agency understanding and uptake of secure cloud services and hasten cloud certification to PROTECTED (potentially modelled

on the US FedRAMP program). This would require additional resources for the Australian Signals Directorate for accreditation services. The Australian Signals Directorate should come back to government with a plan coordinated with the Cyber Security Special Adviser.

- **Embracing Adaptive Government:** The Department of the Prime Minister and Cabinet's ICT Procurement Taskforce should consider the ABS eCensus procurement process as a case study on the barriers and opportunities to delivering better ICT outcomes. This should include developing a more agile approach to market testing and contracting options, ICT procurement skills and outsourcing oversight arrangements.
- **Cyber Security in a Digital First World:** The Digital Transformation Agency, in partnership with the Australian Signals Directorate and the Department of Finance, should:
    - develop a proposal for consideration by the Digital Transformation Committee of Cabinet to create a "cyber security shared services" digital security consulting organisation within the Digital Transformation Agency. This would ensure security is integral to all new online service delivery proposals and facilitate partnering between agencies to draw on cyber security expertise in larger agencies with more mature capabilities.
    - consider how to strengthen central governance and assurance, and this ownership may no longer logically sit with ASD, given their broader portfolio of responsibilities.
    - identify capable agencies and accredit them to deliver shared services for citizen-facing projects where, for higher risk online delivery programs, smaller agencies must partner with (or source their ICT project management from) an identified lead agency or through a core service such as GovCMS.

Recommendations for the Australian Bureau of Statistics

- The ABS should engage an independent security consultant for a wide-ranging examination of all aspects of their information collection and storage relating to Census data – from web application through to infrastructure and policies and procedures.
- The ABS should ensure future significant changes to personal information handling practices are subject to an independently-conducted privacy impact assessment and are supported by broad ranging consultation.
- The ABS should adopt a privacy management plan to enhance its capability to identify and manage new privacy issues.
- The ABS should assess and enhance existing ABS privacy training for staff.
- The ABS should develop a specific strategy to remove the current state of vendor lock-in.
- The ABS should strengthen its approach to outsourced ICT supplier performance management to ensure greater oversight and accountability.
- The ABS should draw upon the lessons it takes from the Census experience to help to guide and to advocate for the cultural change path it is following.

- The ABS's decision in August to assemble an independent panel to provide assurance and transparency of Census quality is supported and the resulting report should be made public.
- The ABS should implement a targeted communication strategy to address public perceptions about Census data quality.

The ABS should report monthly to their Minister outlining progress against the above recommendations.

Better Practice Guidance for Agencies:

- Agencies should review their approach to cyber security incident response planning and coordination and exercising of those plans with stakeholders.
- Agencies should ensure independent security assessments are conducted on critical ICT deliverables.
- Agencies should test security measures and monitoring systems for online government services under foreseeable adverse conditions, including under attack conditions.
- Agencies should be conscious of updated interpretations of governing legislation to addressing the changing technological environment. Agencies should review their oversight and assurance arrangements for outsourced cyber security services.
- The Office of the Australian Information Commissioner has recommended the government develop an APS-wide Privacy Code in collaboration with the Office. The Code should address privacy and security risks by requiring all agencies to:
    - have an up-to-date privacy management plan
    - appoint dedicated privacy contact officers
    - appoint 'Privacy Champions'
    - undertake written Privacy Impact Assessments where relevant, and
    - take steps to enhance internal privacy capability.

PART 1: TRUCK ACROSS THE DRIVEWAY – THE #CENSUSFAIL INCIDENT OF 9 AUGUST 2016

1.1 Incident Timeline

Key findings

- The eCensus suffered a series of preventable outages due to distributed denial of service (DDoS) attacks resulting from a failed geoblocking strategy.
- As IBM attempted to restore the system during the fourth DDoS attack they rebooted hardware and a router failed to restart, further compounding network issues.
- An IBM network performance monitoring system indicated there was unusual outbound traffic from the eCensus system and IBM was unable to conclude whether it was malicious (data exfiltration or compromise) or benign.
- The ABS decided to close the eCensus to the public out of concern relating to the unusual outbound traffic.
- It was later determined there was no unusual outbound traffic from the system.
- Australians filling in their Census forms online did not cause a failure of the system; submission rates were in line with the ABS's expectations and well within load capacity.

In a snapshot...

At 8.09pm on 9 August the Australian Bureau of Statistics (ABS) closed the *2016 Australian Census of Population and Housing* (eCensus) form to new submissions because it feared data exfiltration was occurring. The ABS judged that the inconvenience of temporarily preventing new submissions was preferable to the risk or perception that data had been exfiltrated or compromised.

Throughout 9 August, the eCensus suffered a series of outages as a result of four distributed denial of service (DDoS) attacks. These outages were preventable and resulted from a failure on the part of the company contracted (IBM) to build and run the eCensus system to deliver on its contractual DDoS protection obligations. In addition, the DDoS attacks suffered by the ABS on the day were relatively small (between 1.5 and 3 gigabytes (GB)/second (s)). In comparison, another major Australian government website has, on more than one occasion, been subjected to DDoS attacks of around 20GB/s without that site suffering an outage.

In responding to the fourth DDoS attack, IBM discovered it was unable to log onto the routers at the IBM end of the links with the Internet Service Providers (ISPs). The routers were rebooted and one of the routers could not reload its configuration due to incorrect register settings, so IBM loaded the configuration manually.

During the fourth attack and after the router failure, an IBM network performance monitoring system indicated there was outbound traffic from the eCensus system and IBM was unable to conclude whether it was malicious or benign.

A DDoS attack is designed to disrupt or degrade an online service by flooding the system with traffic, consuming and diverting resources needed to support normal operations. A DDoS attack is not a hack, a breach, or a compromise, where data are exfiltrated or altered. However, while DDoS attacks do not trigger risk of exfiltration, they can be used as a cover to divert attention and resources while exfiltration is attempted.

The outages were not caused by Australians filling out the eCensus. In fact, the loads on the eCensus system were tracking according to predictions.

Those responsible for the DDoS attacks have not been identified. The Australian Federal Police is investigating the incident at the request of the ABS. But attribution of malicious actors online is difficult and denial of service incidents are hard to trace.

There is no indication that the Census data collected by the ABS is insecure or was compromised.

The technical detail

At 10:10am on 9 August, the eCensus system experienced the first of a series of DDoS attacks (around 3 GB/s). This attack lasted 11 minutes and was small by government standards. The eCensus system was unavailable to the public between 10:16am and 10:21am.

At 10:30am the ABS and IBM held discussions about the appropriate response to DDoS attacks.

The ABS and IBM agreed that a planned mitigation, known as 'Island Australia', which blocked all non-Australia IP addresses (geoblocking) would be implemented to deal with any future attacks. IBM recommended, and ABS agreed, that if 'Island Australia' was implemented it would be kept on until at least midnight. IBM was responsible for invoking this mitigation.

At 11:45am a second DDoS attack of a similar magnitude occurred, and the system was again unavailable to the Australian public.

Two minutes after this attack started, IBM called Telstra and NextGen, as the ISPs to the IBM data centre, to request implementation of geoblocking. This mitigation worked and the eCensus was once again available to the Australian public.

At 11:55am the ABS reported the two DDoS attacks to the Australian Signals Directorate and sought advice to counter any further attacks.

At 3:06pm ASD provided written advice to the ABS, which included

recommendations to:

- report any suspected DoS/DDoS traffic from cloud services to their established abuse-reporting mechanisms;
- consider shifting IP addresses in order to defeat IP-based targeting; and
- block unused protocols as far upstream as possible.

At 4:12pm the ABS Information Technology Security Advisor distributed the ASD advice to relevant ABS and IBM staff. The advice was considered and actioned where practicable:

- Cloud service providers were made aware of the abuse; and
- Other mitigations were discussed with IBM, but it was not considered possible to make changes while the system was live.

At 4:52pm a third DDoS attack occurred which was completely mitigated because geoblocking was in place and worked as intended. Australian public use of the eCensus was not disrupted.

At 7:28pm a fourth DDoS attack occurred, which by 7:33pm had again rendered the eCensus system unavailable to the Australian public. Two factors caused this blockage:

- geoblocking did not function as intended; and
- the nature of the malicious traffic was different from the three previous attacks, with an additional attack component degrading the eCensus system faster.

By this time approximately 2.3 million Australians had successfully completed the eCensus. **Figure 1** demonstrates that eCensus form submission rates were in line with ABS expectations, well within load capacity, and did not cause a failure of the system.

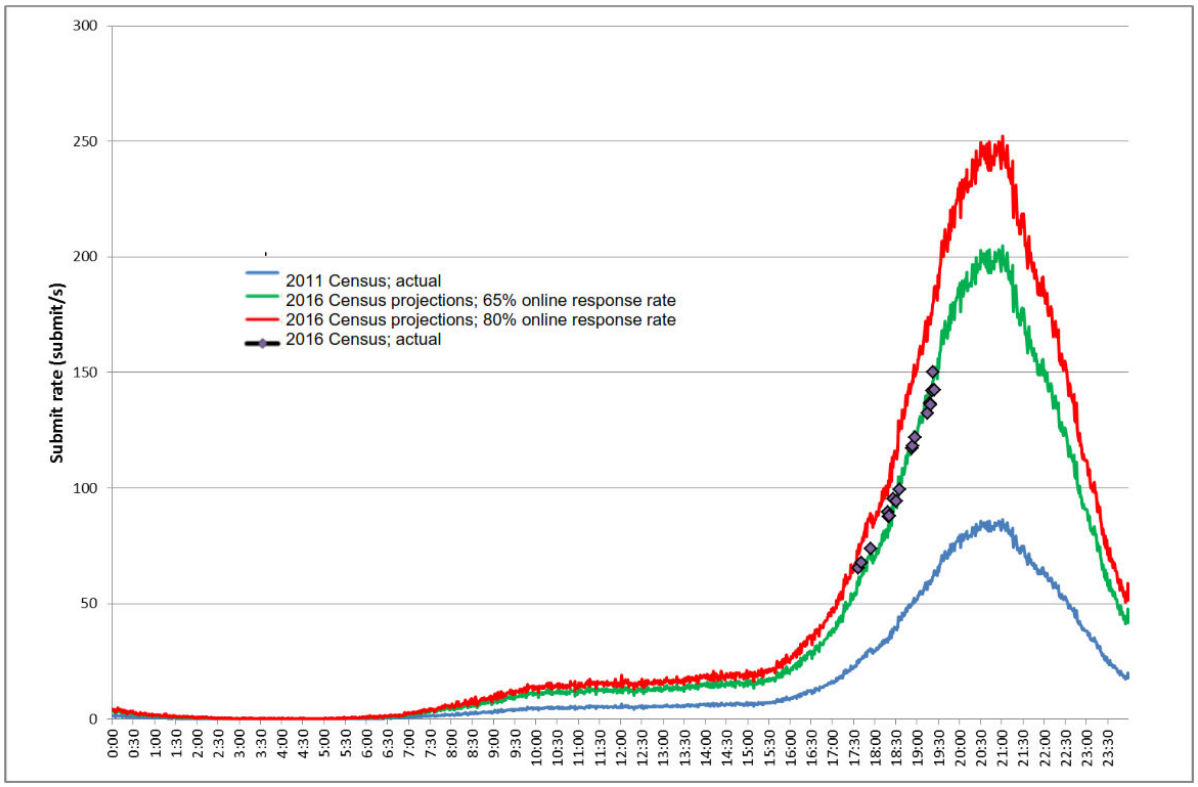


Figure 1. *eCensus* submission rates projected versus actual - *Australians attempting to complete Census online forms did not cause a failure of the eCensus system: Census online form submission rates were within expected and tested-for limits.*

This DDoS was similar to the previous attacks except an additional attack, or by-product of the attack, was encountered: in addition to DNS reflection traffic, the eCensus web servers began experiencing resource-exhaustion issues as all available HTTP worker threads were occupied. The total amount of attack traffic was 1.5GB/s, of which 500Megabytes/s reached the eCensus platform.

The eCensus infrastructure began experiencing DDoS conditions as a large amount of network traffic began to affect both the eCensus application servers and upstream network infrastructure.

Because the eCensus was experiencing problems, the ABS requested that IBM enable 'overload' mode on the application which prevented new users from starting their Census forms.

As a result of the DDoS traffic IBM was unable to log onto remote routers. This failure initiated a train of investigation, including contacting the ISPs to confirm geoblocking was still in place and to explore why it was not effective against this attack.

At 7:43pm IBM made attempts to reboot the system. The reboot caused a router at the IBM end of the Telstra link to lose its settings. The router would not reload its configuration from disk. Later analysis on the problem router identified that it was not faulty. Rather, the settings that IBM had configured on the router prevented it from loading its configuration after a reboot. An additional router was acquired and was available as a cold spare the next morning.

Around the time that the evening DDoS activity started, and the router had

failed, IBM and the ABS observed an unusual spike in outbound traffic in the IBM network performance monitoring system (the IBM dashboard was visible to IBM and the ABS). This was not a security monitoring system, but IBM was unable to explain the spike, which prompted concerns that eCensus data was being exfiltrated or compromised.

IBM and the ABS prioritised identifying the cause of this unusual traffic.

Key decision: At 7:45pm, with concern high that the eCensus data needed to be protected, and still no clearer understanding of the 'unusual' traffic in IBM's network performance monitoring system, Chris Libreri (the ABS General Manager, Census and Statistical Network Services Division), took the decision to close the eCensus to the Australian public. The eCensus was closed to the Australian public at 8:09pm.

At 7:57pm the ABS outlined to ASD the issues the eCensus system was experiencing. ASD advised to:

- work with upstream providers;
- follow the guidance provided earlier in the day; and
- follow ASD's 'Preparing for and responding to DDoS activities' *Protect* product.

IBM's attempt to reboot the system at 8:20pm failed.

Key decision: At 9:15pm the ABS determined to keep the eCensus form closed until it was confident it understood:

1. the 'unusual' outbound traffic patterns in IBM's network performance monitoring system;
2. why geoblocking failed to protect against the fourth DDoS attack; and
3. that protections against any new DDoS attack would be effective.

This decision was collectively taken by: David Kalisch (Australian Statistician), Jonathan Palmer (Chief Operating Officer, ABS) and Chris Libreri (General Manager, Census and Statistical Network Services Division).

At 2:00am on Wednesday 10 August, the ABS and IBM (with concurrence from ASD) conclusively determined that the unusual traffic in the network performance monitoring system was not malicious. Apparent traffic had, in fact, spiked due to network issues, and no actual increase in outbound traffic had occurred. The most likely explanation for this is that, due to network connectivity issues, the so-called 'spike' was due to delays in the monitoring system receiving performance data resulting in increased reported outbound traffic.

Further details:

- IBM ran through its analysis of the suspicious spike in outbound traffic and IBM identified it as a false alarm.
- IBM analysis was that no actual outbound traffic occurred. The networking issues being experienced caused their network performance monitoring system to report a spike in outbound traffic based on incomplete information.
- To investigate this issue, IBM pulled network monitoring and log data from each of the Census application tiers, as well as the network provider logs, to check whether this outbound spike was seen elsewhere. IBM could not identify this activity elsewhere.
- ASD agreed with IBM's analysis and that IBM's analysis was thorough, noting that ASD itself did not conduct any analysis of raw data or logs.

Meanwhile, efforts continued to address the other two concerns – the failure of geoblocking and the effectiveness of further DDoS protections.

On the afternoon of Wednesday 10 August, as investigation continued into the failure of IBM's 'Island Australia', IBM, on advice from ASD, put in place additional DDoS mitigation efforts.

Investigation subsequently confirmed that NextGen's upstream provider, Vocus, did not have properly-configured geoblocking in place, a failure which allowed international traffic to reach the eCensus. This failure was compounded by the fact that Vocus also peered with Telstra, creating a **single point of failure**. The high level network diagram at **Figure 2** outlines this arrangement.

Compounding the problem, NextGen did not have its DDoS attack mitigation service enabled for IBM's data centre. It is probable that IBM had not requested activation of that service. NextGen utilise the services of a security vendor to provide attack mitigation and detection services, but they had only enabled the detection service on this occasion.

The reasons for attack mitigation not being fully enabled are unclear, which further highlights the inadequacies in risk management and governance for the Census Project.

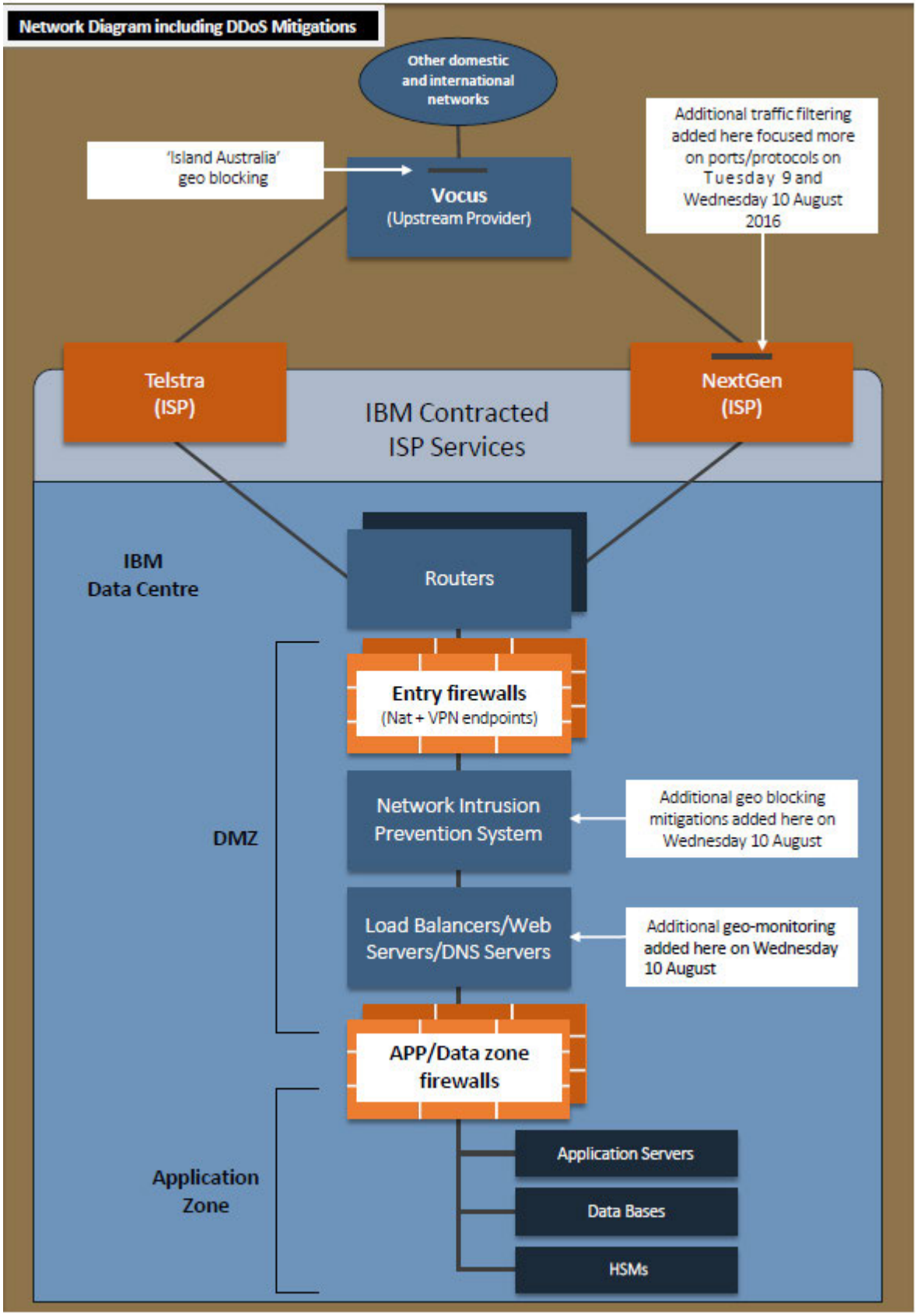


Figure 2. *High level network diagram.*

At 6:30pm on Wednesday 10 August, while the eCensus form was closed to the Australian public, a fifth DDoS attack occurred. The additional mitigations that had been put in place rendered the attack unsuccessful.

ASD technical and management staff worked with the ABS to understand the events and what was required by the ABS and IBM to get the system back online. The ABS, ASD and IBM discussed the significantly increased likelihood of further denial of service attacks due to the global media coverage of the incident.

By 1:16pm on Thursday 11 August, based on a technical assessment of the additional mitigation strategies deployed by IBM, ASD was of the view that IBM had taken all steps that could reasonably be taken in the time available to support a reactivation of the ABS Census website.

At 2:29pm on Thursday 11 August the eCensus form was reopened to the Australian public, 1 day 18 hours and 44 minutes after the decision to close the eCensus form.

1.2 Incident Management

Key findings

- The ABS had no clearly identified and tested cyber security incident response processes. The result was ad hoc decision making.
- The ABS's crisis communications were inadequate, and engagement with Ministers, stakeholders and the public was not timely.
- ASD did not provide timely notifications to the Australian Cyber Security Centre (ACSC) partner agencies nor to PM&C, in its capacity as the lead cyber policy agency.
- The government's Cyber Incident Management Arrangements policy was not adequate in providing guidance in managing the Census incident.

Recommendations:

- **Crisis Communications and Coordination:** The Department of the Prime Minister and Cabinet should strengthen cyber security incident management arrangements across government and ensure the policy is widely circulated, well understood and regularly exercised. This includes:
    - incorporating lessons learned from the eCensus incident response into the Cyber Incident Management Arrangements (CIMA);
    - ensuring effective crisis incident notification and coordination arrangements across Australian Cyber Security Centre agencies and between the Australian Cyber Security Centre, the Crisis Coordination Centre and the Department of the Prime Minister and Cabinet;
    - developing communications strategies, with key talking points for a range of cyber security incident scenarios; and
    - developing a whole-of-government 'cyber security lexicon' to assist with clear and consistent communication relating to cyber security issues.
- **Education:** The Attorney-General's Department should develop a "Cyber Bootcamp" for senior government executives and Ministers as part of the Cyber Security Strategy Awareness program. The Bootcamp would educate participants about cyber security fundamentals and how to talk about issues with the public and be aligned to Data61's work with the Australian Institute of Company Directors.

Better Practice Guidance for Agencies:

- Agencies should review their approach to cyber security incident response planning and coordination and exercising of those plans with stakeholders.

Planning for the worst... or not?

The ABS and IBM had a library of at least six incident management documents to guide them through Census night.

The guides ranged from general to specific, and covered key decisions makers, points of contact, mechanisms for collaboration between the ABS and IBM and a high level overview of an incident response process.

None of the documents outlined a comprehensive cyber incident response plan

to be followed on Census night.

Crisis plans existed but appear not to have been fully tested, nor were they consulted when most needed

The number of documents prepared was not practical and even when looked at collectively; they do not adequately provide guidance in key areas such as thresholds for escalation of incidents and processes for communicating to Ministers and other government departments.

The documents suffered from inconsistent definitions, unclear processes, a lack of focus on cyber incidents and an absence of thorough testing.

The documentation provides a definition of Denial of Service (DoS) as well as Distributed Denial of Service (DDoS) as types of cyber security incident which may impact the eCensus and suggests that the online Census being compromised by a virus or prolonged denial of service attack would constitute an operational crisis.

The documents do not address the 'Island Australia' geoblocking concept and how and when it would be implemented as a response measure. 'Island Australia' is noted as the appropriate response to a DDoS attack in a draft unapproved IBM document, however the status and intended use of this particular document is not clear.

Census night: cyber security incident management

The ABS's documentation detailed that 'overload' mode could be used to close the website to the Australian public through preventing new users from logging onto the Census while allowed users already logged on to complete their session. 'Overload' mode was to be used in response to critical problems that could not be addressed through standard means. It is further documented that if the implementation of this mechanism is due to a hardware failure, it is expected that it would remain in place until the fault is rectified. The decision to implement, and continue using, this mechanism on Census night was in line with the purpose outlined in the ABS's planning documentation.

Escalation thresholds were not clear, nor were obligations and coordination mechanisms across key stakeholders

The ABS's incident management documentation did not identify an escalation threshold for notifying ASD in the event of a cyber security incident. The documentation suggested that ASD could be contacted if it is necessary to escalate any security concerns. The contact details listed were outdated, referring to the Cyber Security Operations Centre (CSOC) rather than the Australian Cyber Security Centre (ACSC). This suggests a lack of effective communication between the two organisations.

The ABS first contacted ASD at 11:55am on Census day to report the early two DDoS attacks and to seek advice to counter any potential further attacks. The notification to, and a request for assistance from, ASD at this time was appropriate as IBM and its ISPs were providing DDoS mitigation support to the ABS. The ABS drew on ASD's expertise, requesting advice on any additional mitigation techniques that could be used to prevent further DDoS attacks. The advice ASD provided was based on generic and existing information as opposed to investigation of specific factors of the ABS's network that may have caused it to be susceptible to DDoS attacks. The ABS's request was consistent with ASD's role to provide advice and assistance to government agencies on matters

relating to the security and integrity of information.

The subsequent requests the ABS made to ASD for assistance on Census night reflected a lack of prior agreement about crisis arrangements, and highlighted misunderstanding by the ABS about the level of support ASD could realistically provide. For example, the requests included:

- ASD provide resources to assist the ABS and IBM to investigate the anomalous outbound traffic identified on the eCensus system (without an understanding of 'normal' traffic, ASD staff would be of minimal use).
- ASD staff attend IBM's Baulkham Hills facility in Sydney where the eCensus was hosted.

The ABS and IBM expected ASD could be called upon to identify the cause of, and to fix, the identified issues. Such assistance was not possible as ASD did not have an established understanding of the systems being used. A clear understanding of the roles and capabilities of both ASD and the ABS should have been obtained prior to Census night.

The ABS's expectations of ASD resulted in an interpretation of ASD's advice as assurance on key matters. For example, the ABS Director IT Security advised the Australian Statistician that ASD had concluded the unusual outbound data reported by the IBM network performance monitoring system was a false positive. ASD did not independently develop this conclusion: using information provided by IBM, ASD agreed with ABS and IBM's assessment that the unusual outbound traffic was a false positive.

The ABS and IBM did not have a consolidated approach to managing the eCensus incident. IBM requested investigative support from ASD when ASD was already engaged with the ABS. The disconnected approach demonstrates a lack of awareness of the incident response plan, which specified that all engagement with third parties should be handled by the ABS.

The coordination problem was again clear later in the evening when IBM contacted the Australian Federal Police (AFP) for assistance. AFP in turn contacted Australia's Computer Emergency Response Team (CERT Australia), who contacted ASD. The disjointed approach to communications was a combination of inadequate planning which did not fully outline what appropriate communications looked like, and the prepared plans not being followed on the night. A coordinated approach is necessary to ensure that communications and mitigation activities are timely and accurate.

The multiple avenues used by the ABS and IBM for requests to different agencies within the ACSC on Census night highlights the need for the ACSC to provide greater clarity about who should be contacted and under what circumstances. The ACSC should also ensure that ACSC partner agencies are notified in a timely manner to ensure an integrated approach to incident management.

Inadequate cyber security incident policy guidance

The Department of the Prime Minister and Cabinet's (PM&C) Cyber Incident Management Arrangements (CIMA) policy establishes the framework for government's response to cyber security incidents.

The CIMA outlines the roles and responsibilities of specified Ministers and government agencies as part of a coordinated response to cyber security incidents.

The CIMA did not provide appropriate guidance to agencies on Census night and was therefore inadequate: most aspects of the CIMA were not followed; those engaged in the crisis probably never considered it; and the ABS would have been unaware of its existence.

Escalation thresholds and processes are not well defined within the CIMA and are largely focused on impacts to national security, rather than issues that go to availability and confidence in online services or reputational risks. The vagueness of language in the CIMA is much the same as that which plagued the ABS incident management plans. The use of imprecise language across multiple documents demonstrates that appropriate and consistent definitions are difficult. It highlights the importance of getting the language right as incidents will happen.

The Crisis Coordination Centre (CCC) within the Attorney General's Department (AGD) is responsible for monitoring information sources and advising Government of potential crisis management issues. Due to media reporting of a malicious attack originating from overseas against the Census, the CCC issued an incident notification at 7:17am on 10 August 2016. This notification was based on press reporting and without any knowledge of the incident response processes in motion. While the eCensus incident did not meet the thresholds for a crisis response according to the CIMA, notifying the CCC of the ongoing investigation would have enabled consistent messaging across Government.

Australia's April 2016 Cyber Security Strategy identified a core action to update and expand the government's CIMA. This should be accelerated and lessons learned from the eCensus incident incorporated. The CIMA must be disseminated to key stakeholders, tested and reinforced regularly through exercising.

Recommendation:

The Department of the Prime Minister and Cabinet should strengthen cyber security incident management arrangements across government and ensure the policy is widely circulated, well understood and regularly exercised. This includes:

- **incorporating lessons learned from the eCensus incident response into the Cyber Incident Management Arrangements (CIMA);**
- **ensuring effective crisis incident notification and coordination arrangements across Australian Cyber Security Centre agencies and between the Australian Cyber Security Centre and the Crisis**

Coordination Centre and the Department of the Prime Minister and Cabinet;

- **developing communications strategies, with key talking points for a range of cyber security incident scenarios; and**
- **developing a whole-of-government 'cyber security lexicon' to assist with clear and consistent communication relating to cyber security issues.**

Census night: crisis communications

In effectively dealing with a crisis, an organisation's first response is everything. Communications must be quick, accurate and consistent. The ABS's communications response was none of these.

The ABS's crisis communication plans exhibited three main shortfalls:

1. Critical government and political stakeholders that would need to be engaged or informed in a crisis were not identified or consulted in the lead-up to the Census.
2. Detailed response planning (processes and procedures) were not outlined for a range of potential adverse events. Nor were they circulated or agreed to by key stakeholders – Ministers and other government agencies.
3. Crisis messaging (draft holding lines, talking points, social media posts and website holding pages) for a range of adverse events were not developed.

The failings in the ABS's handling of the events surrounding the eCensus not only damaged its reputation but also impacted community confidence in the Government's ability to deliver and manage online services. This set-back will have wide-ranging consequences for Government. Selling the idea that we are ready for a new digital era just got a lot harder.

Better Practice Guidance for Agencies:

Agencies should review their approach to cyber security incident response planning and coordination and exercise those plans with stakeholders.

The ABS failed to inform key stakeholders…

The ABS did not proactively inform their Minister that the eCensus had been closed to the public.

A lack of crisis communications planning was evidently clear in the way ministers and the public were informed

At 8:22pm on Tuesday 9 August, around 50 minutes after the eCensus outage commenced, the ABS's responsible Minister, the Minister for Small Business Michael McCormack tried unsuccessfully to contact David Kalisch. The Minister then tried to call the Census 2016 Program Manager, Duncan Young.

At 8:26pm, David Kalisch returned the Minister's call and provided an initial briefing of the situation. This was the first communication the ABS had with the Minister about the DDoS attacks

At 8:32pm, Minister McCormack contacted the Prime Minister, and a minute later, the Treasurer.

At 9:26pm, the Secretary of the Department of the Prime Minister and Cabinet called the ABS and received a briefing.

At 10:02pm and 11:15pm, David Kalisch called the Treasury Secretary to provide a briefing.

At no point during the evening or the following morning did the ABS's Communications team contact other government agencies to notify them of the issue. Nor did the ABS provide key stakeholders, including Ministers, with talking points to ensure consistent messaging was being given to the public.

At 1:00am on Wednesday 10 August, the ABS prepared a brief on the incident which was shared with representatives from the Treasurer's Office, The Treasury, Minister McCormack's office and the Secretary of PM&C ahead of an interagency teleconference scheduled for 5:00am.

Due to an administrative error the Prime Minister's Office did not receive this brief until 4:57am.

At the 5:00am meeting talking points for senior officials and ministers were developed and a media strategy agreed.

Following the meeting, David Kalisch used the information in the ABS brief as background for two early morning ABC radio interviews he conducted. This information was not provided to PM&C line areas, their media teams, or other government agencies.

A further meeting occurred at 8:00am to brief the Prime Minister, Minister McCormack and the Treasurer and agree the approach for a press conference, which occurred at 10:40am. Prior to the press conference, PM&C led the drafting of whole-of-government talking points.

The first version of whole-of-government talking points was disseminated by PM&C Media at 11:04am on 10 August 2016, followed by a second version with a progress update at 6:35pm that evening.

Notifying the public

At 8:09pm, 36 minutes after the eCensus became unavailable, the ABS published a 'high volume' message to the Census webpage.

> *"Please be advised that the 2016 Census online form is currently experiencing high volumes. Please try again in 15 minutes."*

This has since been criticised for its inaccuracy as the website was not experiencing unexpectedly high volumes of legitimate traffic. In fact, this erroneous message only served to fuel public speculation that the site had collapsed under the weight of too many Australians filling out the eCensus at the same time.

Iterations of the following message were then posted to Facebook at 8:37pm,

tweeted at 8:38pm and published on the website at 8:41pm:

> *'The ABS and Census websites are currently experiencing an outage. We are working to restore the service. We will keep you updated.'*

Around 40 minutes later, the Census website was updated:

> *'The ABS and Census websites are currently experiencing an outage. We are working to restore the service. We will keep you updated.*

At 10:58pm ABS posted the following on Facebook (and a similar tweet):

> *The ABS and Census website are unavailable. The service won't be restored tonight. We will update you in the AM. We apologise for the inconvenience. There will be no fines for completing the Census after August 9. There's still plenty of time to complete the Census. Thanks for your patience.*

The ABS and Census webpages were updated with the same message 15 minutes later, and a media release was issued at 11:24pm, which also noted that ABS staff would not be available for interviews and a further statement would be provided in the morning.

The ABS severely underutilised social media as a communications tool to keep the public informed of the incident. Their lack of timely and transparent communications lost them trust, and opened the door to speculation.

At 5:50am on Wednesday 10 August, David Kalisch conducted a live interview with ABC News Radio. He conducted another interview a short time later with ABC Radio National.

At 6:00am, the ABS were instructed by Minister McCormack's Office to:

- play a support role;
- not proactively engage with media; and
- direct all media enquiries to the Minister's Office.

At around 7:30am the ABS took to Facebook and Twitter to confirm "the eCensus was subject to four DDoS attacks of varying nature and severity". Subsequent tweets provided further detail:

> *Steps have been taken during the night to remedy these issues, and we can reassure Australians that their data are secure at the ABS.*
>
> *After the fourth attack, just after 7:30pm, the ABS took the precaution of closing down the system to ensure the integrity of the data.*
>
> *The first three caused minor disruption but more than 2 million Census forms were successfully submitted and safely stored.*
>
> *Fines will not be imposed for completing the Census after Census night.*

ABS would remind Australians that they have plenty of time to complete the Census, to well into September.

At 10:40am, the first press conference took place, attended by Minister McCormack, David Kalisch and Alastair MacGibbon.

At 11:00am, Alastair MacGibbon conducted the first of ten interviews for that day, to clarify the nature of the cyber security incident.

The Prime Minister and the Treasurer conducted a press conference at 11:37am. The Prime Minister thanked Australians who had already completed the eCensus and assured those who hadn't that they would be able to do it safely and securely. The Treasurer further advised that the integrity of the Census had not been compromised and would not need to be re-run.

A number of other Members of Parliament held press conferences and conducted interviews throughout the day, including Christopher Pyne, Richard Di Natale, Bill Shorten, Andrew Leigh, Nick Xenophon and Paul Fletcher.

The ABS also released a number of social media posts and website updates throughout the day outlining that they were 'still working to restore the service'.

On Thursday 11 August, Alastair MacGibbon conducted a further seven interviews before the website was brought back online at 2:29pm, and another two interviews that night.

David Kalisch and Duncan Young held a press conference at 5:15pm on Thursday 11 August following the reactivation of the Census website.

Recommendation:

The Attorney-General's Department should develop a "Cyber Bootcamp" for senior government executives and Ministers as part of the Cyber Security Strategy Awareness program. The Bootcamp would educate participants about cyber security fundamentals and how to talk about issues with the public and be aligned to Data61's work with the Australian Institute of Company Directors.

PART 2: THE LEAD UP TO #CENSUSFAIL

2.1 Cyber Security

Key findings

- ABS preparations for the 2016 Census addressed some security concerns appropriately, but there were gaps. Use of a comprehensive security framework – and independent validation of the security implementation – would have strengthened security planning.
- The Review concluded that the ABS did not have a formal process for accepting responsibility for system security, including identifying and accepting residual risks, a government policy requirement of the Information Security Manual. The ABS disputes this and asserts Census Program Board signed off business risks.
- Protection from DDoS attacks was inadequate and untested.
- Exchanges between the ABS, ASD and IBM suggest a lack of clarity in capacity, roles and responsibility for cyber security across government and with contracted service providers.
- There is no evidence of any weakness that has been exploited to compromise the confidentiality and integrity of the collected data.

Recommendations:

- **Security Framework:** The Australian Signals Directorate should strengthen the framework to help agencies improve the security of their networks:
    - update the Information Security Manual about security measures to protect the availability of online services;
    - in collaboration with the Digital Transformation Agency, lead a 'sprint' to lift agency capabilities to protect against denial of service attacks; this should provide a pilot model for future 'sprints' to build cyber security capacity across the Commonwealth;
    - develop and implement a security framework for high-risk online essential services and special events, to complement the high risk agency security framework identified in the Cyber Security Strategy; and
    - review its model for prioritisation and proactive engagement with agencies to provide cyber security support and develop a service catalogue of offerings to ensure clear understanding of capabilities; this may require additional resources to achieve. The Australian Signals Directorate should come back to government with a plan coordinated with the Cyber Security Special Adviser.
- The ABS should engage an independent security consultant for a wide-ranging examination of all aspects of their information collection and storage relating to Census data – from web application through to infrastructure and policies and procedures.

Better Practice Guidance for Agencies:

- Agencies should ensure independent security assessments are conducted on critical ICT deliverables.
- Agencies should test security measures and monitoring systems for online government services under foreseeable adverse conditions, including under attack conditions.
- Agencies should be conscious of updated interpretations of governing legislation to addressing the changing technological environment. Agencies should review their oversight and assurance arrangements for outsourced cyber security services.

Planning for a secure eCensus

Security featured as a core element of the ABS planning for the eCensus. However, the security planning processes were not sufficiently comprehensive or robust. The ABS and IBM focused on a few areas of security – the confidentiality and integrity of data – while underinvesting in the availability of the system.

The ABS was dependent on IBM to develop and implement the security measures and the ABS did not seek sufficient independent validation that the arrangements were effective. The Review concludes that there was no specific decision taken by the ABS to formally accept the system security arrangements, including identifying risks, mitigation measures and acceptance of residual risk. This process is mandated by ASD's Information Security Manual as a measure to ensure accountability and a final verification of the appropriateness of security measures.

The ABS disputes the Review's judgement and asserts that there are mechanisms for accepting responsibility for system security, including identifying and accepting residual risks and that business risks were signed off through Census Program Board.

No Independent Security Assessment

The ABS Request for Tender included specific requirements for security testing, and for an independent security assessment to be conducted on the application and hosting facilities. The independent assessment was to be performed by an Information Security Registered Assessors Program (IRAP) assessor, the government and ASD-endorsed standard for independent assessment of network security implementation.

IBM agreed to this through their response to the Request for Tender. The assessment was to evaluate the security design of the eCensus solution, including an audit of the firewall rules, physical configuration and connectivity as part of the cutover procedure.

No IRAP assessment took place.

The ABS informed the Review team that it took the decision not to seek an IRAP assessment as, in the context of other assurance activities, it "would not have

provided significant additional assurance". The other assurance activities – outlined in a plan presented to the ABS Protective Security Management Committee on 21st March 2016 included:

- Compliance assessment of the IBM data centre for physical security against Protective Security Policy Framework (PSPF) Zone 4 requirements;
- ASD review of the eCensus system cryptographic architecture;
- Source code review by independent provider Saltbush;
- Penetration testing, also provided by Saltbush; and
- IBM documentation and compliance reviews.

However, these assessments were focused on specific components of the eCensus system and led the ABS to conclude that the system was secure. Further, the ABS did not have a process to identify and accept residual risks.

According to the ISM, the purpose of a security assessment, such as an IRAP assessment, is to determine whether the system architecture is based on sound security principles and to determine whether the security measures chosen have been implemented, and are operating, effectively.

An IRAP assessment would likely have revealed gaps in security planning. An IRAP assessment may have identified that DDoS mitigation was not part of the ABS IT security assessment and therefore would not have been covered by its assurance activities. The ABS disputes this, stating "an IRAP assessment would have been unlikely to identify susceptibility of the system to denial of service attacks". Clearly, we will never know the answer to this, but the absence of an IRAP assessment provided one less opportunity to find fault in the ABS preparations before Census night.

Review of available security documentation

Following the eCensus incident, ASD performed a review of available security documentation. This review assessed available security documents for evidence of the identification and intended application of security controls. The review also assessed the compliance of security controls for which guidance is detailed in the ISM. However, the review assessed only documentation and plans and did not verify the implementation of security controls on the eCensus system.

The review identified that IBM had produced significant volumes of documentation on securing and securely operating the eCensus system and associated data.

In accordance with risk-based security management principles, IBM documented cases of security non-compliance, including non-compliance to the ASD Top 4 security mitigation. In general, most of the IBM documentation was only accepted informally by the ABS, without documented decisions on non-compliance.

In regard to DDoS mitigation, IBM provided some initial advice based on constrained thinking which was primed by the ABS's interpretation of data requirements outlined in the *Census and Statistics Act 1905*. The ABS did not interrogate this advice.

For complete assurance, a comprehensive independent assessment of the eCensus system and architecture should be conducted.

Recommendation:

The ABS should engage an independent security consultant for a wide-ranging examination of all aspects of their information collection and storage relating to Census data – from web application through to infrastructure and policies and procedures.

Better Practice Guidance for Agencies:

Agencies should ensure independent security assessments are conducted on critical ICT deliverables.

Accreditation for policy-sensitive online services

The ISM mandates the development and application of an accreditation framework to all systems. The accreditation process allows for formal recognition and acceptance of residual security risks to a system and the information that it processes, stores or communicates.

The ISM accreditation process includes:

- independent assessments of planned security controls and of the implementation of those controls;
- certification that the security controls are operating effectively based on the assessment; and
- accreditation that the system is ready to operate, on the basis that the security controls appropriately mitigate risk and that residual risk is accepted by the accreditation authority.

For most single-agency systems, the accreditation authority is an agency senior executive; for most multi-agency systems, the accreditation authority is the Department of Finance.

Systems such as the eCensus system occupy a new space; single-agency systems that, due to their profile, incur whole of government risks. Risks associated with this new space will be further compounded where smaller agencies, such as the ABS, have limited access to technical and risk management expertise.

The 2016 Cyber Security Review found it is difficult to assess the cyber security effectiveness of Government agencies. Existing measurement tools largely rely on self-reporting and focus on compliance, rather than on the effectiveness of risk management strategies. Further, the cyber security capability in agencies is varied, and many agencies are underequipped to deal with the digital age. This appears consistent with the situation in the ABS.

There would be value in a series of ‘sprints’ to assist agencies with core protections and capacity to take them to the next level in secure online service delivery.

Data confidentiality

The ABS and IBM focussed on applying cryptographic protections and system defences to protect the eCensus system and data against internal and external threats. The ABS and IBM sought external advice on key cryptographic controls from ASD, as well as source code review, and penetration testing services.

The data collected via the eCensus system is protected by multiple encryption layers. These include:

- encryption of individual Census responses;
- the data are delivered to ABS using commercial grade encryption (IPSEC Virtual Private Network);
- the data can only be decrypted by the ABS; and
- appropriate hardware and software are used to manage encryption and decryption.

The eCensus system has tools that monitor for network load and performance, which can identify potentially malicious activity. But these are not security systems.

The ABS uses technical and organisational controls to mitigate the risk of unauthorised access to data by ABS staff and contractors. The ABS is an accredited Integrating Authority of the Cross Portfolio Data Oversight Board. This accreditation means the ABS's processes and systems for high risk data integration projects have been independently validated.

Names and addresses collected through the Census are stored separately from other data. Database access is restricted to specific roles within the organisation and no individual working with the data can view the full data set. Access reports are regularly reviewed by ABS.

Prior to the eCensus opening, two penetration tests of the eCensus system were conducted. Additionally, a source code review of the eCensus system was conducted in accordance with the Open Web Application Security Project (OWASP) code review guide. No significant vulnerabilities were identified and no significant risks were left unresolved.

There is no evidence of weakness that has been exploited to compromise the confidentiality and integrity of the collected data.

Data loss detection & network performance monitoring

The decision to close the eCensus system was taken due to an inaccurate monitoring statistic

On Census night, an intrusion detection system alert did not trigger the decision to close the eCensus system. Rather, a network performance monitoring system indicated what appeared to be a spike in outbound traffic. IBM was unable to explain if this was malicious or benign.

The ABS subsequently rendered the eCensus form unavailable to the public due to concerns for the confidentiality of Australians' data.

The DDoS attack, compounded by the incorrect configuration of a router, caused the network performance monitor to indicate unexpected outbound traffic. This indication was due to delays in the monitor receiving performance data and consequently generating incorrect statistics.

Monitoring systems were not tested against adverse conditions

The network performance monitor was not designed to operate under conditions of a DDoS attack or router failure. Under the conditions of an attack, the validity of the reporting was not understood by the IBM security staff. Consequently, IBM staff had to perform a detailed, time-consuming, investigation before they could conclude that the report was incorrect.

Network performance monitoring was not tested under attack conditions, and the limits of its reliability were not understood.

Mitigating Distributed Denial of Service (DDoS) attacks

The ABS and IBM developed a series of mitigations against threats to availability of the eCensus system

The ABS contracted IBM to develop mitigations against threats to availability of the eCensus system – including specific measures intended to mitigate DDoS attacks.

Clearly, these measures did not work.

The ABS identified the threat of DDoS attacks. When it engaged IBM as a contractor, the threat was expressed in the *Statement of Requirements for the 2015* eCensus *solution* which was issued with the RFT on 25 July 2014.

IBM's response to the ABS's RFT included a number of security measures to protect the hosted solution from DoS attacks:

- *the ability to block IP addresses and ranges at the entry firewall, and the entry router;*
- *the ability to block source IP addresses and ranges at the [Border Gateway Protocol (BGP)] gateway, and at the Internet Service Provider (ISP) end of the BGP link through negotiation and tools provided by the ISP vendor;*
- *a negotiated agreement to block all international access to the eCensus solution when requested ('Island Australia'); and*
- *engagement of a DDoS mitigation service from an external provider. ([IBM contracted ISP]).*

These mitigations were unusual but if implemented as conceived, the mitigations would have been sufficient to prevent the outage on Census night

An internal IBM document produced in July 2016 contains IBM's plans for detecting and responding to operational events, including a DDoS incident. **Box 1** shows that the sole IBM response action for a DDoS attack was the 'Island Australia' strategy.

Box 1: IBM eCensus 2016 Operational Issues Recognition and Response Strategy

Security Events

Attack vector: DDoS (large scale distributed attack)
Recognition: ISP alert, ISP bandwidth out of spec, HTTP server out of spec, Firewall CPU utilisation, XGS CPU/Connects/Out of spec, SOC identifies many overseas IPs
Response: Island Australia (Block all international traffic). Too many IPs to block individually.

Attack vector: Denial of service (overload attempts)
Recognition: IPS alert, HTTP server (CPU)
Response: Block IP addresses at firewall

On Census night, 'Island Australia' was the key mitigation employed by IBM to defend the eCensus system from DDoS attack. This involved using geoblocking: a process where all traffic from a specific origin – overseas – is routed into a 'black-hole' and discarded before it reaches the target system.

The ABS should have requested clarification from IBM about the DDoS mitigation service to be used so that the ABS understood how the hosted solution would be protected. But at the time, the ABS tender evaluation team believed that the DDoS mitigations offered by IBM were sufficient.

On 24 March 2016, Mr Jonathan Palmer (Deputy Statistician, ABS) emailed IBM and ABS colleagues following a demonstration of the online form. The email referenced questions Mr Palmer had asked IBM at the demonstration, about resilience to DDoS attacks and "whether IBM experience is that our architecture has proven resistance [sic] to attack by Anonymous."

On 12 April 2016, an internal ABS email, sent at 12:53pm, summarised IBM responses around 'phishing and DDoS attacks' and stated:

At a high level, our architecture resists DDoS attacks via use of multiple layers of security. An attack by an actor, such as Anonymous, would need to successfully breach the following layers to reach our web servers:

WWW => Census border firewall => Network Intrusion Protection Service => Host Intrusion Protection Service agent => web server

In general terms, our experience is that most external DDoS attacks are stopped at the border firewall or, increasingly, in front of it, as cloud services are more widely utilised. The 2016 Online Census uses IBM SoftLayer cloud services for key web-facing elements such as content and email delivery.

Between November 2014 and April 2016, multiple risk-workshops were held. DDoS mitigations were considered in each of these as part of the overall risk management plan.

It was the responsibility of IBM to implement the agreed DDoS risk mitigation plan.

On 26 April 2016, the Risk Management Plan (developed by IBM in conjunction with the ABS to identify the risk management processes that would operate in the 2016 Online Census Program) lowered the residual risk likelihood (see Box 2).

Box 2: Risk Management Plan: DDoS risks (summary of table)
Risk: Loss of system availability through a 'technical' Denial of Service attack – noted as possible likelihood with major impact and high exposure.

Risk management approach is to mitigate as noted below. IBM assessed the residual likelihood as unlikely with residual impact as Major and residual exposure as Medium.
Existing security architecture controls:
- web application security testing
- penetration testing
- IBM Security Operations Centre monitoring
- ABS has engaged ASD

Risk: Loss of system availability through a Distributed Denial of Service attack – noted as possible likelihood with major impact and high exposure.

Risk management approach is to mitigate as noted below where they assessed the residual likelihood as unlikely with residual impact as Major and residual exposure as Medium.
Existing security architecture controls:
- web application security testing
- penetration testing
- IBM Security Operations Centre monitoring
- ABS has engaged ASD
- ISP specific measures

IBM's assessment in the Risk Management Plan that the residual likelihood of loss of system availability was unlikely, gave rise to a false sense of confidence that DDoS mitigations would be effective. IBM DDoS mitigations were also not independently verified by the ABS.

Between 6 and 30 June 2016, Revolution IT was engaged to carry out load testing. It covered all ABS IT systems for the Census enumeration, including the IBM Online Census system. Importantly, load testing does not test for DDoS, it is based on legitimate traffic modelling.

The ABS did not receive a summary report from Revolution IT at the time, rather they had a range of test results that were documented and reported on and continued until the platform had passed all necessary tests. Revolution IT staff members worked within the ABS IT environment, with the ABS load test manager and IBM to complete all the necessary load tests and document results.

Constrained thinking?

The ABS and IBM did not conduct thorough testing of one of the key DDoS mitigation techniques utilised on the night

While the initial documents state that DDoS mitigations were planned, including engagement of a mitigation service from an external provider, the final Solution Architecture – describing the system as delivered – states:

> *ISP based DDoS prevention services are not viable as these would be likely to trigger on the normal census traffic profile given its single event peak and lack of build-up period.*

Telstra advises that this description of ISP-based DDoS mitigations is not accurate. Unless there was a design or capacity problem, legitimate traffic would not trigger the DDoS protection service.

ISP-based DDoS mitigation services can also be designed to trigger on particular rule sets (for example, the type or rate of attack). Therefore an ISP-based DDoS mitigation service would likely have at least partially mitigated the DDoS attacks on Census day and would not have affected legitimate traffic.

While there may be additional factors supporting the decision to not use ISP-based DDoS mitigations, there is no record of this being examined.

It is the understanding of the Review that the ABS initially applied a 2011 interpretation of the *Census and Statistics Act 1905* to the 2016 eCensus System. This interpretation required that only ABS staff should be able to access encrypted or unencrypted respondent data.

This requirement may have prevented consideration of commercial DDoS mitigation services. Using a commercial service would require encrypted – or in some cases, unencrypted – respondent data to be analysed by a service provider and judged non-malicious.

While this analysis by the DDoS mitigation service provider would in most instances be automated, the service provider would have privileged access to the systems that perform the analysis. With privileged access, an employee of the service provider may be able to – intentionally or unintentionally – access Census respondent data, breaching the 2011 interpretation of the *Census and Statistics Act 1905*.

Consequently, it is likely the legislative interpretation constrained procurement options for DDoS mitigation. The ABS disputes this conclusion.

Better Practice Guidance for Agencies:

Agencies should be conscious of updated interpretations of governing legislation to addressing the changing technological environment. Agencies should review their oversight and assurance arrangements for outsourced cyber security services.

The 'test'... and then the real test

It is clear that the mitigations failed and were inadequately tested; however it is not clear why the mitigations failed

'Island Australia' was tested but not until four days before Census night, when the eCensus system was already live and open for form submission. The timing was chosen to represent the optimal traffic profiles for plan validation, whilst minimising the risk of impacting the respondent-user experience.

The testing was limited – IBM simply activated 'Island Australia' for 10 minutes and monitored the system for international traffic while IBM tried to access the system from overseas.

IBM and the ABS's documents indicate a mismatch between the risk, the intended mitigation and the implementation of the 'Island Australia' strategy.

eCensus system documentation describes plans to apply the 'Island Australia' mitigation for short periods, in the order of 10 minutes, to mitigate an individual attack. On Census day, however, IBM suggested – and the ABS agreed – to apply 'Island Australia' indefinitely following the second DDoS attack at 11:47am. Akamai Technologies' 'State of the Internet' report identified an average DDoS attack duration of 16.14 hours in Q1 2016 which suggests that testing for 10 minutes is inadequate.

On Census night, multiple ISPs encountered problems with the implementation of 'Island Australia'. The incorrect implementation resulted in no alerts for specific IP addresses and some international routes not being blocked. Consequently, the DDoS continued without immediate identification despite real-time monitoring and the implementation of the 'Island Australia' mitigation.

Additionally, 'Island Australia' was implemented on Census night for multiple hours without prior testing of the impacts of prolonged implementation.

The ABS and IBM should have conducted additional and more thorough testing of the implementation of 'Island Australia'. Testing should have:

- involved all ISPs;
- included testing of the integration with other mitigation techniques to be used; and
- been conducted over a longer time period.

NextGen's upstream provider, Vocus, did not have properly-configured geoblocking in place, a failure which allowed international traffic to reach the eCensus. This failure was compounded by the fact that Vocus was also the upstream provider for Telstra, creating a **single point of failure**.

Adding to the problem, NextGen did not have its DDoS attack mitigation service enabled for IBM's data centre. It is probable that IBM had not requested activation of that service. NextGen will utilise the services of a security vendor to provide attack mitigation and detection services, but they had only enabled the detection service on this occasion.

The reasons for attack mitigation not being fully enabled are unclear, which further highlights the inadequacies in risk management and governance for the

Census Project.

Could 'Island Australia' have worked?

If implemented as conceived, 'Island Australia' would have defended against DDoS attacks originating from overseas. The strategy, however, was unusual, and did not provide mitigation against attacks using traffic originating from within Australia.

Black-holing and geoblocking, as used in 'Island Australia', are acknowledged in the security community as possible mitigation for DDoS attacks. But they are not necessarily the best option. One leading network equipment company describe black-holing as "not a solution."

Geoblocking is not a part of ASD's advice.

Further Issues

In available documentation prepared by IBM and the ABS, no consideration is given to the impact of geoblocking on the eCensus system.

Parts of the eCensus system – including the Softlayer mail relay used for password resets – are located offshore, and hence the eCensus system would not function as intended while 'Island Australia' was active.

Additionally the access point to the internet for a number of Australians – including Vodafone customers located in NSW or those using VPNs – is via an international location. Those affected would have been unable to use the eCensus system while 'Island Australia' was active without explanation as to why.

Better Practice Guidance for Agencies:

Agencies should test security measures and monitoring systems for online government services under foreseeable adverse conditions, including under attack conditions.

Did the ABS get the support it wanted and needed?

The ABS engaged ASD for advice and assistance with the eCensus system in late 2014, after entering into the contract with IBM.

Between December 2014 and March 2015, the ABS engaged a specialist area of ASD for evaluation of some cryptographic protections of the eCensus system.

There was a disconnect between the advice and assistance ASD offered and the advice and assistance the ABS sought to receive

In March 2015, a second area of ASD contacted the ABS offering technical security assessments. In the exchange which followed, the ABS incorrectly interpreted that ASD was offering the ABS a service – a source code review – that ASD was neither offering nor resourced to perform. However, as the ABS had passed documents to ASD, the ABS may have incorrectly surmised that these documents were assessed by ASD and no cause for concern was found. ASD indicates that it was waiting for further, detailed, documents and took no action. This exchange petered out in October 2015 without clear resolution.

Later, in March 2016, the area of ASD responsible for coordinating

relationships, advice and pro-active assistance to government agencies contacted the ABS to discuss threats to the eCensus system and establish points of contact and processes in the event of a cyber security incident. This third area of ASD was, when the offer was made, unaware of the prior engagement between ASD and the ABS.

By March 2016, no substantive changes could be made to the eCensus system, nor could technical assessments be carried out in time for Census night.

Later correspondence, up to and including on Census night, indicates an ongoing disconnection between the advice and assistance ASD sought to offer and the advice and assistance the ABS sought to receive. For example, on Census night IBM and the ABS requested ASD send Sydney-based incident responders to the IBM facility to assist with investigations.

ASD documents indicate that the organisation is stretched to capacity. While ASD has world-class technical experts, they are spread across many tasks and ASD has too few coordination staff to facilitate external relations. Well-meaning offers of assistance are not internally coordinated and consequently advice and assistance are not targeted for greatest effect.

Lastly, neither ASD nor the ACSC are assurance organisations, tasked with proactively engaging agencies. If asked specific questions by agencies they do their best to answer and assist. The ABS, on the other hand, would fairly conclude that it had engaged with ASD and that such engagement provided certain levels of assurance, even when none was given or implied by ASD.

Recommendation:

The Australian Signals Directorate should strengthen the framework to help agencies improve the security of their networks:

- **update the Information Security Manual about security measures to protect the availability of online services;**
- **in collaboration with the Digital Transformation Agency, lead a 'sprint' to lift agency capabilities to protect against denial of service attacks; this should provide a pilot model for future 'sprints' to build cyber security capacity across the Commonwealth;**
- **develop and implement a security framework for high-risk online essential services and special events, to complement the high risk agency security framework identified in the Cyber Security Strategy; and**
- **review its model for prioritisation and proactive engagement with agencies to provide cyber security support and develop a service catalogue of offerings to ensure clear understanding of capabilities; this may require additional resources to achieve. The Australian Signals Directorate should come back to government with a plan coordinated with the Cyber Security Special Adviser.**

2.2 Privacy

Key findings

- The DDoS attack against the online Census system did not involve the compromise of personal information of Australians.
- The closure of the eCensus website appears to have amplified existing community concerns about security and privacy in relation to the eCensus - concerns which originated from an ABS decision to extend retention of name-and-address information for up to four years in the 2016 Census.
- The ABS led its own privacy impact assessment (PIA) on the decision to retain name-and-address information. The PIA identified the likelihood of each privacy risk eventuating, post risk-mitigation, as 'very low' and did not consider the wider privacy implications of the move to a 'digital first' Census. The engagement of an independent consultant, as done by the ABS in 2005, could have altered these assessments.
- While the ABS approached the Office of the Australian Information Commissioner (OAIC) and State and Territory Privacy Commissioners about the proposal to retain names and addresses, public consultation on the proposal to retain name-and-address information failed to attract community attention. And the ABS accepted this.
- The ABS has a number of well-developed privacy practices and procedures to manage personal information in an open and transparent way, and published its PIAs. But opportunities exist to improve the robustness of its privacy framework.
- The Census incident provides an opportunity for government agencies to learn from the ABS experience and reaffirm their commitment to the protection of privacy, and to enhance public confidence in government data linkage and online service delivery. The OAIC has suggested this could be achieved through a Privacy Code.

Recommendations

- The ABS should ensure future significant changes to personal information handling practices are subject to an independently-conducted privacy impact assessment and are supported by broad ranging consultation.
- The ABS should adopt a privacy management plan to enhance its capability to identify and manage new privacy issues.
- The ABS should assess and enhance existing ABS privacy training for staff.

Better Practice Recommendations for Agencies:

- The Office of the Australian Information Commissioner has recommended the government develop an APS-wide Privacy Code in collaboration with the Office. The Code should address privacy and security risks by requiring all agencies to:
    - have an up-to-date privacy management plan
    - appoint dedicated privacy contact officers
    - appoint 'Privacy Champions'
    - undertake written Privacy Impact Assessments where relevant, and
    - take steps to enhance internal privacy capability.

A Commitment to Privacy

This incident offers valuable lessons for future Government projects that rely on personal information as a core input of data-innovation or data-sharing projects

The ABS decision to shut down the eCensus website on 9 August was made to protect the privacy of Australians. The decision ensured that the DDoS attacks against the eCensus system, and concern over the network load monitoring system's unexplained outbound traffic, did not involve the compromise of Australian personal information.

The decision demonstrated the ABS's commitment to upholding the privacy, confidentiality and security of the personal information it collects.

However, the closure of the website and the discussion about cyber attacks amplified significant community concerns about the retention of name-and-address information collected during the 2016 Census.

Certain shortcomings appear to have restricted the ABS's ability to recognise the significance of managing the perceived community concerns with equal fervour as managing the eCensus technical controls.

The impact of the privacy concerns illustrates how privacy issues can escalate rapidly and cause significant reputational damage for agencies, endangering the viability of key government projects.

Unless the Australian Public Service responds to the Census incident appropriately, the public stands to lose confidence in key government projects which rely on the use of personal information. This setback could jeopardise the success of future projects which seek to realise the value of data in Australia's digital future.

Was the process by which the ABS decided to retain name-and–address information robust?

The ABS decision to extend the retention of name-and-address information from 18 months to up to four years was made after a lengthy period of internal consideration, a privacy impact assessment (PIA) process, and public consultation conducted over three weeks. Decisions made during each of these processes impacted upon the rigour of the overall assessment of privacy concerns.

Organisations can elect to conduct a PIA without the assistance of external stakeholders. But an independent PIA can help identify privacy impacts that may not be obvious to agency staff.

The ABS decision to conduct the privacy impact assessment internally restricts its ability to offer the same assurances that an independently-conducted PIA could have

Further, an independent PIA can help an organisation to develop community trust in the PIA findings and the project's intent.

The ABS Data Integration Section developed the PIA. The section had experience in managing data-integration projects and had developed PIAs for those projects, consistent with the ABS Data Integration Policy. The PIA process was overseen by the Census Program Board, Data Integration Committee and the Executive Leadership Group - the final decision maker on the PIA and proposal.

In contrast, in 2005 the ABS engaged an independent consultant to undertake a PIA into proposals for the 2006 Census. By failing to seek independent advice in 2016, the ABS could not demonstrate the same level of effective separation between the PIA drafter and ultimate decision-maker.

Veracity of privacy analysis

The 2015 PIA identified five 'privacy risks' for the Census project:

1. Unauthorised access by ABS staff to data stored in the ABS environment;
2. Unauthorised non-ABS access to data stored in the ABS environment;
3. Accidental release of name and/or address data in ABS outputs or through loss of work-related IT equipment and IT documentation;
4. Reduction in participation levels in ABS collections due to loss of public trust; and
5. 'Function creep' – unintentional expanded future use of retained name-and-address information.

The likelihood of each of these privacy risks eventuating, post mitigation strategies, was assessed as 'very low' by the ABS, as was the extended retention of name-and-address information.

Post risk-mitigation, the 'very low' assessment of the loss of public trust in the 2015 PIA was significantly lower than previous ABS risk assessments. An October 2015 internal ABS paper identified the un-mitigated risk of privacy concerns on 2016 Census participation levels as high risk (likelihood - possible, impact – major). The 2015 PIA subsequently discussed a number of mitigation strategies to address the potential reduction in Census participation levels.

Scope of the PIA

The PIA demonstrated that the retention of name-and-address information was permitted and protected by the *Census & Statistics Act 1905* and the *Privacy Act 1988*. Whilst the PIA recognised the need to maintain community trust to undertake the 2016 Census, it did so from a security and legal compliance perspective. As such, the PIA did not capture the implications of the shift to a

'digital first' Census.

Consideration of the shift to digital first offered an opportunity for ABS to promote the benefits of the digital Census. In particular, an online Census form has significant privacy benefits over traditional paper forms. Promotion of these benefits could have engendered greater community confidence in the security of the 2016 Census. The decision not to undertake an analysis of the broader implications of the 2016 Census – instead relying on the broader analysis done in the 2005 PIA – meant that the opportunity to assess contemporary privacy considerations was not seized.

Public consultation

The ABS determined that the 2015 PIA would be the primary vehicle for external engagement and communication in relation to retention of Census identifiers. The ABS approached all State and Territory Privacy Commissioners for comment on the PIA and met with the OAIC. The public consultation – between 11 November and 2 December 2015 – did not receive significant media coverage or community attention. Only two news articles mentioned the proposal, and only three community members provided submissions to the ABS – each raised concerns with the proposal. No defined time period is required for a PIA public consultation process. However, consideration should be given to the significance of the proposal when determining the time period.

During discussions between the ABS and OAIC, a number of issues were discussed on the content of the PIA. Importantly, the OAIC does not comment on the project (or policy objectives/proportionality) that is being considered by a PIA. Rather, the OAIC highlights issues that a business owner may like to consider as part of the PIA's development. As a result of these conversations, the draft PIA was amended before being published.

A PIA should not be seen as a process that ends with the publication of the PIA report. A PIA may be useful more than once during the project's development and implementation, and as such is considered to be a 'live document'. The 2015 PIA recommended the retention of names and addresses. Despite increased publicity on the Census in the months following that decision, it is unclear whether the ABS revisited its final PIA report. Doing so would have allowed the ABS to consider, in the face of the increased publicity, key decisions relating to the PIA process.

The ABS could have considered whether the original risk analysis of the public perception that the retention period would be indefinite was adequate. The subsequent decision by the ABS in April 2016 to clarify the retention period was one step taken to address this community concern. Furthermore, the ABS could have considered the overall adequacy of its public consultation methodology to quell these perceived concerns around retention.

Recommendation:

The ABS should ensure future significant changes to personal information handling practices are subject to an independently-conducted privacy impact assessment and are supported by broad ranging consultation.

Organisational capability to address the privacy issues for Census 2016

The ABS has strong privacy practices, but gaps in its privacy framework may have impacted upon the organisational awareness of contemporary privacy concerns of the 2016 Census

The ABS has a number of well-developed privacy practices and procedures to manage personal information in an open and transparent way. Despite the strength of these practices, gaps exist in the ABS privacy framework. These gaps appear to have impacted upon the ABS staff awareness of privacy issues in the lead-up to the 2016 Census. Whilst the ABS has already taken steps to address these gaps, additional opportunities exist to improve the robustness of the ABS privacy framework.

Responsibility for privacy matters

The ABS has committed to embedding a culture of privacy that fosters compliance with is legislative obligations. This commitment is led by the appointment of key roles and responsibilities for privacy management:

- A Privacy Officer, supported by a dedicated team, to provide advice to business areas on privacy matters and oversee investigations and reporting on privacy complaints;
- A Privacy Implementation Officer to lead ABS privacy reforms following the amendments to the Privacy Act in 2014; and
- Senior executive staff appointed to key governance bodies that consider privacy and security issues for the ABS.

ABS privacy policy and related information

The ABS has a privacy policy which provides information to the public on the personal information handling practices of the ABS. The ABS also has an internal privacy policy which provides guidance to ABS staff about obligations under the Privacy Act and Census and Statistics Act, and on how to seek privacy advice within the ABS. These policies are supplemented by a specific Census 2016 privacy policy, and a 'Privacy, confidentiality and security' webpage that explains these policies to members of the public.

ABS Policies and Procedures

The ABS has a number of policy and procedural documents that outline how Census staff are expected to handle personal information across the information life-cycle. A 2015 internal audit found that 'the majority of ABS policies and processes in place ensure compliance with the Privacy Act.'

The ABS has updated its policies identified as requiring improvement in the 2015 audit, and has developed new policies where none existed. These developments include documented procedures for receiving and managing privacy complaints.

The ABS has also demonstrated a commitment to 'privacy by design' by mandating the completion of a PIA for all data-integration projects assessed as high-risk.

The current ABS practices and procedures provide a structure for the ABS to meet its legal compliance with the Privacy Act. However those practices and procedures do not provide an adequate platform for ABS staff to move beyond minimum compliance, in order to create a mature privacy management

framework. As such, there remains an opportunity for the ABS to add a privacy management plan to its suite of privacy-related documentation. A privacy management plan is a tool that can assist agencies to improve their privacy processes continuously. Relevantly for the ABS in the aftermath of the 2016 Census, the plan could help to build responsiveness to new privacy issues, including the privacy implications, risks and benefits of new technologies.

Privacy awareness

All ABS staff sign secrecy and fidelity agreements upon engagement with the ABS, and are required annually to resign those agreements. The ABS delivers privacy messages, led by the Privacy Officer, through newsletters and bulletins on its intranet and actively participates in Privacy Awareness Week each year.

The 2015 audit of ABS privacy compliance identified that privacy awareness and training materials were developed to inform ABS staff of the 2014 changes to the Privacy Act. But only a low proportion of staff accessed this material. To address this low participation, in late 2015 the ABS introduced mandatory privacy training for all staff, to be refreshed every two years. Privacy training is a key component of induction to the ABS.

The ABS training material is appropriately tailored to account for the organisational characteristics of the ABS. However, the ABS training material is heavily weighted towards internal compliance with security and confidentiality of personal information. This compliance focus is likely the result of the secrecy provisions within the *Census & Statistics Act 1905* which govern ABS staff.

An opportunity exists for the ABS to assess and enhance its organisational capability to identify and manage both internal and external privacy risks, with a particular focus on its privacy training. Engagement with privacy experts outside of the ABS would offer an additional perspective on ABS privacy training. A multi-agency approach to developing privacy materials could be used to establish the delivery of a consistent, baseline privacy capability across the Australian Public Service.

Recommendations:

The ABS should adopt a privacy management plan to enhance its capability to identify and manage new privacy issues.

The ABS should assess and enhance existing ABS privacy training for staff.

Lessons for all agencies

As the national statistical agency, the ABS is experienced in handling large amounts of personal information. Despite the number of long-standing privacy practices and procedures the ABS has in place to protect that personal information, the Census incident highlighted a number of significant gaps in its privacy capability. This incident offers other APS agencies the opportunity to learn from the ABS experience, and identify and address any APS-wide barriers to the effective management of privacy concerns.

Legislative and policy settings for gathering and linking personal information

Government must support APS agencies to build a strong 'social licence' to use data in new ways, and strengthen the ability of agencies to address contemporary privacy concerns

The policy decisions surrounding the 2016 Census were made in the context of the Australian Government's broader open data policy agenda. The open data agenda is an important component of the Australian Government's broader *National Innovation and Science Agenda*.

The Australian Government has consistently emphasised that appropriate privacy and security protections are key to the success of the broader innovation agenda.

In addition to the obligations in the Privacy Act, the ABS (like many other agencies) is subject to agency-specific laws which modify its obligations under the Australian Privacy Principles (APPs). The ABS is subject to the *Australian Bureau of Statistics Act 1975* and the *Census and Statistics Act 1905*. These Acts give the Australian Statistician powers to approve specific uses of ABS-collected data for purposes (such as research or data integration) that would not otherwise be allowed under the relevant legislative frameworks.

Government agencies therefore have considerable statutory authority to decide when to collect, use and share data. The relevant policy question is therefore *how* agencies should exercise their powers within the legal parameters set for them by Parliament.

Community expectations for mandatory collection of personal information

The Australian community now expects transparency in the handling of personal information. However, the community's expectations are heightened when information is collected compulsorily, and on a large scale.

It is therefore particularly important that agencies such as the ABS, which have the power to compel individuals to provide their data, are as transparent as possible about their data practices. They must clearly articulate the purposes for which personal information is collected and used. Agencies must also be able to point to the public benefits of doing so.

Building a social licence for new uses of data

The Australian community is increasingly aware of privacy issues, especially in light of the ubiquitous availability and use of online services. Most people accept that Australian government agencies will need to use their personal information to provide them with the services they want, or to improve on those services. But, people want to know how their information is being used and what impact this use will have on their lives, particularly when this information is collected compulsorily. When people have confidence about how their information is managed, they are more likely to support those uses of information.

If no social licence exists for new uses of data, agencies will face public backlash if data are mishandled, or where service-delivery failures occur, as the Census incident demonstrated. A real or perceived lack of transparency or public support can pose serious risks to the government's future ability to conduct valuable data-related projects. As seen in the United Kingdom and New

Zealand, good privacy practice, together with effective communication and community-engagement strategies, can ensure that the handling of information is consistent with the community's expectations.

APS privacy risk-management capability

Many agencies (including the ABS) already have a number of well-developed privacy practices in place. As outlined earlier in this Chapter, the ABS conducted a PIA process prior to the 2016 Census in order to determine the risks of the new policy directions adopted. But, limitations in that process meant that the ABS was unable to give meaningful consideration to (or effectively address) community privacy concerns.

In light of the Census incident, the ABS, and the APS more broadly, should enhance its ability to identify and manage privacy risks in a way that maintains and builds public trust for Australia's digital future.

Guidance for new or enhanced uses of personal information

A number of agencies have produced guidance to assist agencies to undertake data projects with appropriate privacy and security safeguards in place. These include the *Public Sector Data Management Project* reports and the *Guidance on Data Sharing for Australian Government Entities.* The Secretaries Board has endorsed the *High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes*. Finally, given its overarching regulatory role of the Privacy Act, the OAIC has produced various pieces of guidance, including a consultation draft of the *Guide to big data and the Australian Privacy Principles.*

These documents all highlight privacy issues and external-perception risks. Despite this formal framework, a number of foreseeable privacy and security risks materialised in the 2016 Census incident. APS privacy capability should therefore be strengthened to enable agencies to assess external privacy risks better in light of today's digital realities.

Lessons can be learned from the relationship between the overarching ABS privacy framework and the management of privacy for Census 2016 to enhance public confidence with privacy in future digital engagements with government.

Recommendation: The Office of the Australian Information Commissioner has recommended the government develop an APS-wide Privacy Code in collaboration with the Office.

The Code should address privacy and security risks by requiring all agencies to:

- **have an up-to-date privacy management plan;**
- **appoint dedicated privacy contact officers;**
- **appoint 'Privacy Champions';**
- **undertake written Privacy Impact Assessments where relevant; and**
- **take steps to enhance internal privacy capability.**

The Australian Government must assure Australians that privacy is a key consideration in the planning and execution of government projects. The development of a Privacy Code would address the privacy risks associated with

data projects involving personal information.

A binding Code would support all Australian Government agencies subject to the Privacy Act when undertaking data projects involving the use of personal information. The Code would make explicit the Australian Information Commissioner's expectations of government agencies' existing obligations under the Privacy Act, creating additional clarity and accountability.

Agencies should have an up-to-date privacy management plan

A Privacy Management Plan would set out, in a systematic way, how an agency intends to implement the requirements of the Privacy Code, as well as the requirements in the OAIC's *Privacy Management Framework*. The Plan should also outline how broader privacy risks (such as external perception risks) will be addressed by the agency.

Agencies should appoint privacy contact officers

Agencies should appoint privacy contact officers. Designated privacy officers will be appropriately trained, and be the first point of contact for advice on privacy matters in their agency. The designated privacy officer should also consult regularly with the Privacy Champion in relation to any privacy issues that arise out of the agency's data activities.

Agencies should appoint Privacy Champions

Agencies should be able to communicate effectively with the public about any new or innovative uses of data. Those agencies must articulate the legitimate public-policy purposes for which data will be used, and realistically gauge and address any community privacy concerns or misconceptions.

Senior officials within Australian Government agencies should be appointed as Privacy Champions to provide cultural leadership and promote the value of personal information. They would also be responsible for providing advice on broader strategic privacy policy issues.

Agencies should conduct written PIAs and keep a register of all PIAs undertaken

Agencies should undertake written PIAs or equivalent privacy risk processes for all high-risk projects that involve the handling of personal information. PIAs should assess the overall proportionality of new proposals, and consider broader external perception risks. A mere 'tick-the-box' approach should not be taken. In addition, agencies should keep a register of PIAs undertaken, and make the register and PIAs available to the Australian Information Commissioner.

Development of privacy training for APS staff

The Privacy Code should require agencies to assess their existing privacy capabilities. In particular, they must be able to respond to community sentiment. Privacy-related learning and development should be strengthened where necessary. The OAIC could assist government agencies in implementing this recommendation by developing an e-learning module in consultation with the APSC.

2.3 Communications Engagement

Key findings

- For the 2016 Census communications campaign, the ABS relied on an old approach to communicate an evolving event in a changing environment. The ABS was neither prepared for this challenge, nor able to adapt appropriately.
- Negative sentiment in the community and media about privacy-specific concerns outweighed the negative reporting on technical issues that resulted from the closure of the eCensus form and magnified tensions. It also made managing the message of the DDoS attack being 'just a disruption or inconvenience' difficult, if not impossible.
- A lack of crisis communication planning led to slow and inappropriate execution of public and stakeholder engagement on Tuesday 9 August and the following days.
- The ABS's handling of the incident highlights the importance of clear and concise language. Early and comprehensive stakeholder engagement and pre-agreed processes for handling and communicating cyber incidents are critical. Neither is possible without the common understanding that clear language provides.

Communications campaign

Communications is driven by purpose – if the purpose is wrong, then a campaign is trying to fix a problem that doesn't exist

In most respects, the ABS had a well formed and prepared communications strategy and approach for an awareness raising campaign for the 2016 Census; but it was focussed on the wrong things. The communications problem they needed to address was not a just awareness of the Census, but rather, the introduction of a 'digital first' approach and the associated barriers to participation – security and privacy concerns.

The ABS failed to adapt its media and communications in response to the public relations storm that was brewing in the weeks prior to the Census regarding privacy and security in both mainstream and social media. Instead, the ABS rigidly stuck to its plans, forgoing crucial opportunities to influence and drive the conversation around the Census.

Effective communication is driven by the *purpose* of the campaign – what must change and who needs to be reached to bring about that change. The communication strategy defines how to capture the attention of the target audiences and to convey compelling campaign messages.

In 2006 and 2011, the ABS ran successful communications campaigns. The 2011 campaign won multiple industry awards and the Census achieved an average response rate of 96.5 per cent. The focus of the 2011 campaign was on illustrating how engaged participation in the Census could have personal benefit to the individual.

For the 2016 communications campaign, the ABS decided to stick to the winning formula used in 2011, implementing a campaign focused on raising awareness of the Census and why people should participate.

But the ABS faced three fundamental differences in 2016:

- The ABS was taking a **digital first** approach, aiming to have 65 per cent of respondents complete the form online.
- The ABS would **retain names and addresses** for up to four years for the purpose of more accurately linking data sets.
- The ABS was working in a new and challenging environment – government services are moving online; concerns around cyber security and **government's use of data** is increasing; and public and media engagement online is exploding.

Benchmarking research conducted in 2016 showed that 95 per cent of the population supported the Census during Census week (78 per cent awareness before the Census), up from 94 per cent in 2011 and 87 per cent in 2006. Census awareness and willingness to participate was at an all-time high (see **Figure 3**).

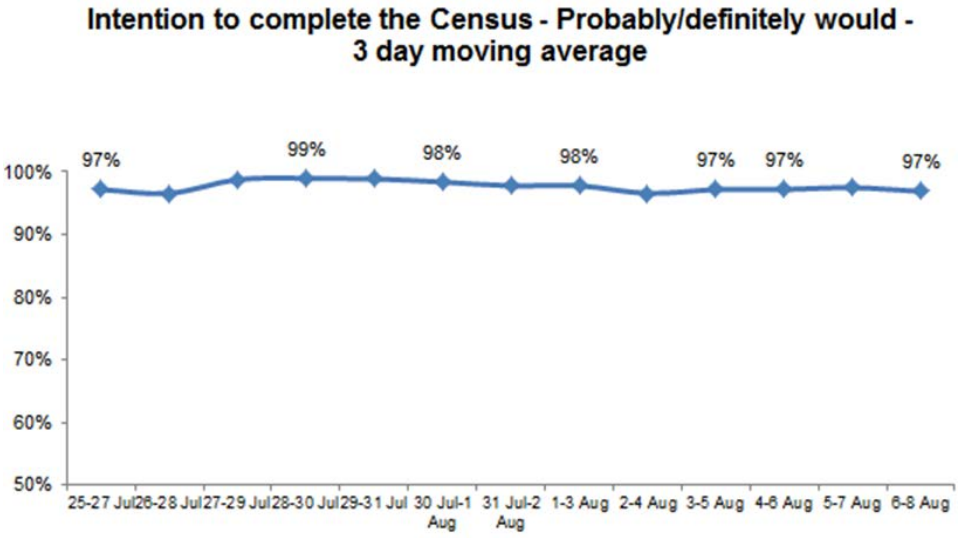


Figure 3: *Intention to complete the Census*

The ABS consistently argues that it needed to address a low level of awareness of the Census and a lack of understanding of the Census. But just as importantly it needed to boost the introduction of its 'digital first' approach and address the associated barriers to participation – security and privacy concerns. Campaign messaging should have focused on encouraging people to 'get online to complete your Census; and your data will be safe with us."

In short, the ABS relied on an old approach (and old messaging) to communicate an evolving event in a changing environment. The ABS was neither prepared for this challenge nor appropriately adapted to it.

Reacting to public sentiment

The media play a central role in informing the public about issues, shaping public opinion and impacting the construction of public belief and attitudes towards change.

In late October 2014, the ABS Executive Leadership Group agreed that the

privacy impact assessment (PIA) process would be the "primary vehicle for external engagement and communication in relation to the retention of Census identifiers [names and addresses]." The ABS announced public consultation regarding privacy via a media release issued on its website, with a submission period of only four weeks – 11 November to 2 December 2015 (just before Christmas).

Media advocacy is a powerful tool to get a message across, but for it to work, you must be engaged and in tune with community sentiment so you can react appropriately

The ABS received only three public submissions. Not only should this low response rate have indicated to the ABS that its public engagement on the key issue of privacy was inadequate, it also left a huge vacuum with regard to capturing public concerns. So the ABS missed an opportunity to identify how to evolve its communication plans developed following qualitative research in 2014 to address more up to date concerns.

As a result, the ABS was ill-equipped to manage the impact changes in the Census would have on a small but important segment of the population and their willingness to complete the eCensus online.

In January 2016, seven months out from the Census, the first articles raising concerns about privacy and security of data appeared in the media. More substantial rumblings began in March, with two main themes emerging:

- That the Census was intrusive and no longer anonymous
- The Census was vulnerable to hackers.

The ABS prides itself on the constant measuring of public sentiment and awareness using traditional survey techniques (see **Figure 4, page 53**). The Review concludes that these surveys contributed to a false sense of security and failure – still at time of writing – to grasp the significance and power of social media groundswells.

Major shifts in public statements regarding the security of the Census began the week prior to Census night, culminating in Senator Nick Xenophon and several other parliamentarians issuing warnings about security and privacy concerns and apparent implementation problems leading to a 'debacle.'

Prior to the closure of the eCensus form, over 11,000 individual mentions (social and mainstream media) were published voicing concerns about the privacy and security of the eCensus. The closure of the eCensus resulted in 17,730 privacy related mentions, far outweighing mentions (1,200 total) of the technical issues experienced – i.e. what happened (see **Figure 4**).

This coverage created overwhelming 'noise' making it difficult for the ABS to remain on message.

The ABS's planned communications were being drowned out. But rather than trying to adapt its approach to limit the impact the reporting had on the public sentiment toward the Census, the ABS stuck to planned messaging ignoring the public relations storm brewing around them.

The failings of the ABS to address issues of concern in the media extend to its use of social media. Analysis conducted on ABS Twitter and Facebook accounts shows that at no point did the ABS significantly change its planned posting schedule or content as a result of critical media reporting

(shown in **Figure 5, page 54**) and of considerable online chatter around privacy (**Figure 4**). The ABS did change its social media advertising as well as engage posters directly on social media. But this was not enough.

The ABS's virtual absence from the privacy and security debate is reflected in its social media crisis escalation matrix – the process designed to monitor, escalate and handle social conversations. The matrix had two main flaws:

1. The ABS's 'qualifiers' (thresholds that had to be met to raise concern) were too high. A 'red level scenario,' the highest categorisation for negative conversation, was enacted only if someone had 10,000 plus followers or a post had over 30 engagements.
2. The ABS's response/action for a 'red scenario' was to hold all social media communications.

The ABS's social media strategy was too restrictive and didn't allow enough flexibility to respond to changing trends in media and social media. As a result, the ABS missed crucial opportunities to inform the conversation around privacy and security and the benefits of the digital first approach.

When public discourse was rising on the issues, the ABS should have been on the front foot addressing these concerns. Key spokespeople should have been conducting interviews, issuing media releases and engaging on social media to drive the conversation and shape the debate.

While the ABS did eventually start engaging in the mainstream media, it was too little, too late. And on the whole the ABS steadfastly stuck to its communications plans, allowing the media, and subsequently the public, to take the lead role. The ABS failed to insert itself in the conversation and underutilised mainstream and social media as a vehicle to shape the debate around the benefits of a digital first approach.

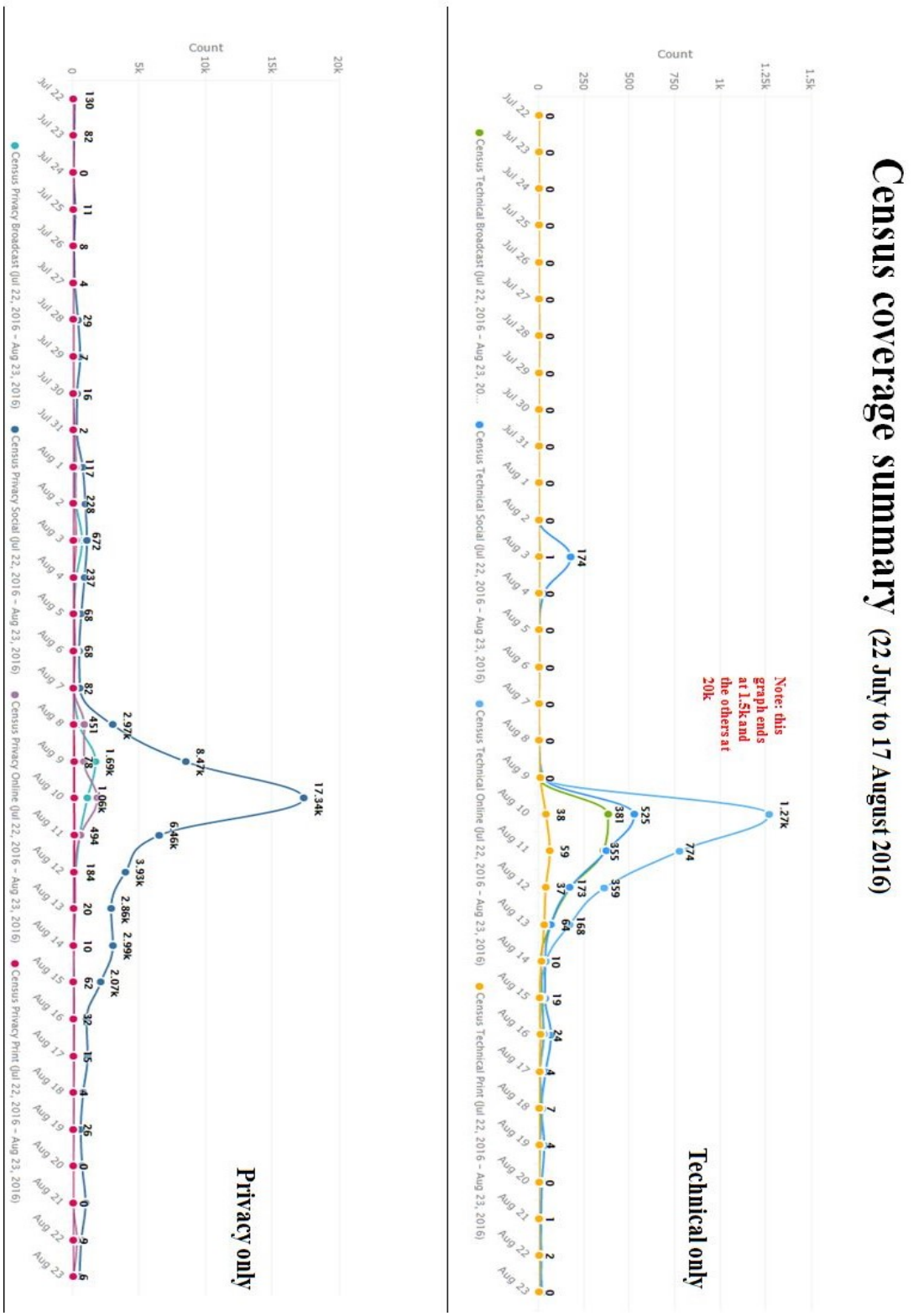


Figure 4: *Census Media Coverage Summary*

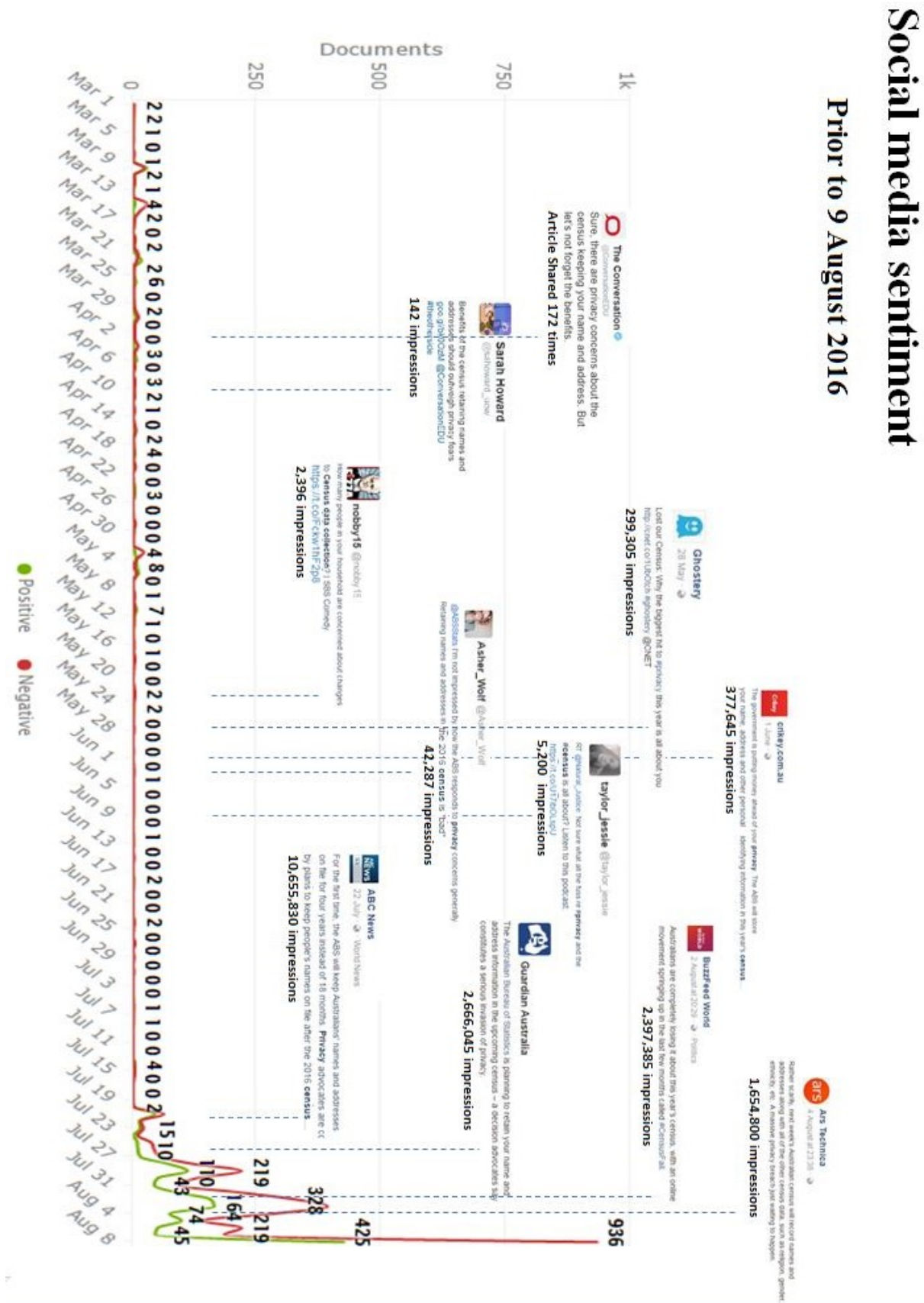


Figure 5: *Social Media Sentiment*

2.4 Procurement, Contracting and Governance

Key findings

Procurement

- ABS procurement practices with the eCensus fell short. While process may have been followed, it appears to have been a compliance exercise rather than striving for the best procurement outcome.
- The ABS did not conduct an open approach to market to invite all potential suppliers to participate in its procurements as it prepared for eCensus in 2011 and 2016. The ABS did not test the market for these procurements and did not use an effective competitive procurement process to ensure that it received the best solutions and value for money.
- The ABS exhibits a repeating trend to cite tight timelines and dependency on current solutions as reasons for sourcing only from IBM.
- Trust, technology dependence and time constraints influenced the retention of ABS's outsourcing provider IBM as a "locked-in" vendor.
- With no market testing/open approach to market since 2008, the ABS limited its opportunity to access better solutions.
- The ABS held the unrealistic assumption that a supplier who performed well in the past would perform well in the future, even when the scope of services has changed.
- The ABS value for money assessment, based as it was on pricing offered solely by the incumbent, lacked rigour.
- ABS's scrutiny and the independent security assessment of the security solutions put forward by IBM were inadequate.
- Census is a foreseeable event that happens at regular intervals and stronger procurement planning will alleviate the pressure each time a solution is sourced from the market.

Governance

- ABS's outsourcing efforts were influenced by its trust relationship with IBM. Independent verification as to DDoS protection mitigations, and to other IBM assurances.
- The ABS did not have an effective IBM outsourcing oversight framework and program in place which meant that the risk ownership and appetite of the ABS appeared limited.
- The ABS did have a risk management plan in place. The ABS considered the risks and mitigation strategies around Census delivery. But it did not consider the risks and mitigation strategies around IBM as the outsourced operator or supply chain, beyond standard strategies being in place to manage the risk.

Recommendations:

- **Embracing Adaptive Government:** The Department of the Prime Minister and Cabinet's ICT Procurement Taskforce should consider the ABS eCensus procurement process as a case study on the barriers and opportunities to delivering better ICT outcomes. This should include developing a more agile approach to market testing and contracting options, ICT procurement skills and outsourcing oversight arrangements.
- **Creating a Positive Risk Culture:** The Department of Finance should assist agencies to actively engage with cyber security risk by developing guidance for managing risk in ICT and cyber security outsourcing.

ABS-specific recommendations:

- The ABS should develop a specific strategy to remove the current state of vendor lock-in.
- The ABS should strengthen its approach to outsourced ICT supplier performance management to ensure greater oversight and accountability.

A cosy partnership...

The ABS rated IBM a 'ten out of ten'

The ABS and IBM enjoyed a close and trusting working relationship. The ABS ranked IBM's performance for the original eCensus in 2006 'ten out of ten' in an independent customer-satisfaction survey commissioned by IBM in September 2006.

The 2011 eCensus Project Completion Report attributed the success of the project to the skills and experience of the people involved in both the ABS and IBM, "and the trusted partner / one team attitude taken by both organisations." The report added that in a recent survey the ABS showed its satisfaction with IBM's performance for the Population eCensus solution and Agricultural eCensus solution with 10 out of 10 for both components. This relationship probably led to the ABS being more trusting of IBM's solutions, based on the assumption that IBM had performed well in the past and would continue to perform well in the future, despite the fact that the scope of services had changed.

Procurement practices evidence a repeating trend: tight timelines and dependency on current solutions as a reason for sole sourcing

The ABS engaged IBM in September 2008 for the supply of the 2011 Data Capture and eCensus systems through direct sourcing. The business case supporting direct sourcing from IBM was prepared in April 2008 and highlighted a number of issues regarding ABS's dependency on IBM and the time pressure it was working under, despite the fact that the Census itself was a foreseeable event.

The ABS judged that several Census applications developed since 1998/9 integrated tightly with IBM's Intelligent Forms Processing (IFP) product suite, and that Census processes developed were completely reliant on the combination of IFP and ABS applications. As a result, a change of supplier would not be compatible for existing systems and would require significant re-work and extensive testing if a new solution were to be adopted.

The business case advised that should the Delegate reject the proposed direct sourcing approach, the timeframe to complete the tender process would be extremely tight and would significantly increase the level of risk. The Delegate,

Jenine Borowik, then General Manager of Technology Services Division, approved the business case in April 2008.

… leading to vendor lock-in

The Commonwealth Procurement Rules (CPRs) are issued by the Minister for Finance under section 105B(1) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). As a non-corporate Commonwealth entity, officials at the ABS must comply with the CPRs when performing duties related to procurement.

In conducting procurements, officials are expected to manage risk. This management requires considering the approach to procurement, evaluating available courses of action and documenting relevant decisions. When making decisions, officials have an obligation to be aware of their responsibilities to make proper use of public resources under the PGPA Act and must achieve value for money in procurement.

In February 2012, the ABS issued an approach to market via a Request for Expression of Interest (EOI) for software and hardware capabilities to accelerate the acquisition and collection of data.

The evaluation report of the EOI was submitted to Jenine Borowik, then First Assistant Statistician of Integrated Collection and Dissemination Services, for approval on 6 July 2012. The report noted that 21 companies responded to the EOI, but these responses did not add any advantage over current ABS solutions. The report recommended that Blaise, the current eForm solutions, be further explored, to enable the ABS either to opt on further developing its current solutions or to conduct an open approach to market.

The ABS did not consider if it had adequate and appropriate ICT capability to undertake the work. Two years later, it became clear that the Blaise solutions could not scale to the requirements of the Census in 2016, leading to the decision to outsource the development and support of the eCensus solution to IBM.

In February 2014 the ABS commissioned an independent assessment of the ICT capability for the 2016 Census. The report found that the ABS did not have sufficient capability in house and recommended engaging an external partner for the eCensus solution. The report also provided advice that only IBM would be able or willing to develop on to the existing eCensus solution, with other companies likely to provide new solutions. The report recommended ABS consider a select tender with IBM for the eCensus solution as the primary option for reducing risk.

A procurement plan prepared in June 2014 proposed approaching only IBM citing the same reasons for a single source approach as in September 2008: dependency on IBM and time pressure. The procurement plan was approved by Patrick Hadley, Chief Information Officer, on 20 June 2014. In September 2014, the ABS again engaged IBM through limited tender, a similar approach as direct sourcing which involved no market testing, this time for the supply of the 2016 eCensus and Data Capture.

Market testing provides an agency insight into available new or better solutions the industry has to offer

In both cases, the ABS applied Section 10.3e of the Commonwealth Procurement Rules as the reason for conducting a limited tender. This particular section deals with situations where

> *"for additional deliveries of goods and services by the original supplier or authorised representative that are intended either as replacement parts, extensions, or continuing services for existing equipment, software, services, or installations, where a change of supplier would compel the agency to procure goods and services that do not meet requirements for compatibility with existing equipment or services".*

Based on the procurement plans, time pressure, rather than perceived technology dependency, was the reason for sourcing the solutions only from IBM. The applicability of this exception rule to these circumstances is debatable. The Census is an activity which occurs at a regular interval, with a long lead-time between each occurrence. Better procurement planning would have alleviated the time/resource pressure when the solution was sourced. Market testing would have provided the ABS with insight into available new or better solutions the industry had to offer. This information would be helpful to ABS in developing a strategy to reduce its dependency on legacy or ageing infrastructure.

Recommendation:

The Department of the Prime Minister and Cabinet's ICT Procurement Taskforce should consider the ABS eCensus procurement process as a case study on the barriers and opportunities to delivering better ICT outcomes. This should include developing a more agile approach to market testing and contracting options, ICT procurement skills and outsourcing oversight arrangements.

ABS-specific recommendation:

The ABS should develop a specific strategy to remove the current state of vendor lock-in.

Assessing value for money

On 23 September 2014, Patrick Hadley, Chief Information Officer, approved the spending proposal for the 2016 eCensus solution which recorded the value for money assessment conducted for IBM's bid. The ABS requested IBM to provide pricing for various eCensus take-up levels (50 per cent, 65 per cent and 80 per cent) and two security models to match the 2006 and 2011 ABS security requirements. New features were costed separately to enable the ABS to eliminate low-priority pieces of work if desired. The ABS then used the information to make a comparison with the spend on the 2011 eCensus.

The ABS was satisfied that the result showed value for money, in that a 3.9 per cent reduction in costs from 2011 to 2016 was attained with an overall improved application outcome. The shortcoming of this approach was the fact that IBM was the sole source of pricing information for both the 2011 eCensus solution and 2016 eCensus solution, which weakens the rigour of the value for money assessment.

Outsourcing is okay, but you still own the risk…

The ABS trusted IBM to deliver…

The ABS had established a strong trust partnership with IBM. As a result, the ABS became reliant and dependent on IBM. The ABS did not have an effective means of monitoring and assessing IBM as an outsourced service provider and therefore did not measure, monitor, and control the enterprise risks, including cyber security risks, represented by the contracting arrangement.

…leading to a lack of independent verification of risk assessment and mitigation

The ABS relied upon the formal contract to deliver outcomes and provide for all contingencies. The ABS did not check thoroughly and monitor that effective cyber security controls were in place with IBM and its supply chain.

For example, when IBM said that their DDoS test was completed and that the protection was effective the ABS did not further gain assurances that the scope and criteria of the testing were sufficient. The ABS also did not require a formal report to be issued with the outcomes. IBM's assurances were taken at face value: if IBM said in an email that DDoS protections worked, the ABS took comfort. The ABS provided minimal challenging or inspection, and did not use third parties to test and verify that DDoS protections were actually in place and effective.

An oversight program would have ensured that IBM and its suppliers and/or supply chain delivered the quality of services required by the contract. The monitoring program should have targeted the key aspects of the contracting relationship with effective independent monitoring techniques. The program would have monitored the IBM service provider environment, including its security controls and the impact of any external events.

This framework would have addressed the IBM outsourced relationship from an end-to-end perspective, including establishing requirements, strategies and a risk management plan.

IBM contributed to the operational risks of the ABS which affected other risk areas:

- Reputation risks—the ISP's failure to implement adequate DDoS protection plans for key processes impaired the ability of ABS to provide critical Census online services to the public; and
- Strategic risk— closing off the eCensus based on inaccurate information from IBM caused the management of the ABS to make poor strategic decisions.

In not monitoring IBM as an outsourced operator the ABS effectively shifted responsibility for these activities to IBM due to:

- The business critical nature of the decisions being taken; and
- The ability to drive changes in risk (including cyber risk), control and compliance practices now rested with IBM.

These activities should ideally remain the responsibility of the ABS Chief Risk Officer (CRO) who reports to the Executive leadership group, the Standard Audit Committee, and other risk committees. A reassessment and a more

independent view of IBM's outsourced risk profile may have ensured a more rigorous risk management process into IBM's contract terms than was required for a medium- or low-risk rated supplier.

Recommendation:

The ABS should strengthen its approach to outsourced ICT supplier performance management to ensure greater oversight and accountability.

From risk analysis to risk management

Census Program Risks were reported and oversighted by the Census Program Board

Although the ABS had documents, meetings and committees focused on risk, and might therefore regard itself as compliant with appropriate risk management methodologies, its actual management of risk with an outsourced provider was poor. The ABS had in place a range of processes for managing risk, including security risk, aligned with the ABS Risk Management Framework (RMF). The ABS 2016 Census Program Risk Register, presented to the Census Program Board on 23 June, specifically called out the risk of security breach, with DDoS attack identified as one source. However, the impact of security risks being realised appears to have been underestimated:

- Reduces online Census participation rates;
- Reduces response rate to the Census, and ABS survey program;
- Increases operational costs due to increased field staff follow up;
- Impacts overall Census data quality;
- Reputation impacts if significant for both ABS and IBM;
- Loss of data; and
- Release of data.

Risk consequence assessment was underestimated

The risk of a security breach was assigned an inherent risk rating of 'extreme' (the highest rating in the ABS RMF) based on a 'likely' (will probably occur) likelihood and a 'severe' consequence (not defined in the ABS RMF). This impact assessment didn't seem to reach broadly enough, to the national level consequences that followed realisation of the risk.

The planned controls to reduce the 'extreme' rating included:

- Operations monitoring with strong alerting and response procedures,
- Good programming practices that reduce risk of incidents,
- Validation of vendor solution for security controls,
- Engaging with external experts such as ASD and vendor security advisors for threat monitoring and controls, and
- Sign off role for all security reviews accepting any residual risks identified.

The control effectiveness rating was assessed as 'good' resulting in a residual risk rating of 'moderate' ('unlikely' consequence; 'major' impact) and attracting periodic monitoring arrangements.

In hindsight, we know that the identified controls were not adequately

implemented for DDoS.

The 2016 online Census Risk Management Plan - dual-badged to the ABS and IBM, but owned by IBM – specifically identifies DDoS risks and associated planning. Loss of system availability via a 'technical' or distributed denial of service attack is identified as 'possible' in likelihood, 'major' in consequence and 'high' exposure. The mitigating controls including:

Risk processes 'ticked the box', but didn't drive security implementation

- Existing security architecture controls:
    a. web application security testing;
    b. penetration testing ; and
    c. IBM Security Operations Centre monitoring.
- ABS has engaged ASD, and
- ISP specific measures.

reduced the assessment to 'unlikely' in likelihood, 'major' in consequence and 'medium' in exposure.

In both these instances of risk planning, the high initial risk ratings do not appear to have driven a resultant focus on the effectiveness of implementation of the identified controls. Nor do they appear to have shaped preparedness for incident management and potential supporting communications strategies on Census night.

Recommendation:

The Department of Finance should assist agencies to actively engage with cyber security risk by developing guidance for managing risk in ICT and cyber security outsourcing.

2.5 A Lesson in Culture

Key findings

- Culture matters. And the culture of the ABS identified by the APSC in 2013 — insular, inward looking, reactive — affected decisions and performance as the ABS planned and carried out the 2016 Census. Moreover, its reliance on past patterns to guide future strategies doesn't work.
- The ABS has been slow to recognise the importance of whole of government engagement.
- In recent years, the ABS has devoted energy and resources to aggressively address the cultural issues highlighted in the APSC Capability Review. The Census incident highlights that the ABS will remain exposed and its effectiveness compromised the longer it takes to achieve its goal of transforming its organisational culture.

ABS-specific recommendation:

- The ABS should draw upon the lessons it takes from the Census experience to help guide and to advocate for the cultural change path it is following.

Organisational culture

"...a degree of organisational isolation and insularity that needs to be addressed." – APSC Capability Review Nov 2013

No one decision or action in isolation stands out as the primary cause of the 2016 Census incident. But it would be a mistake to conclude that ABS's established patterns of behaviour – its culture – had no part to play in Census preparations, the outage and the management of the incident.

As Lynelle Briggs observes in relation to the ABS's handling of changes to the Labour Force Survey in 2014.

> "When [organisations] fail at their core business, it is often symptomatic of underlying cultural and governance problems."

Prevailing culture can be identified in actions and decisions taken to prepare for the 2016 Census that date back to June 2012. Many seem innocuous and almost all are compliant with established government practice. In many ways, the ABS is seen as an exemplar of established government practice: ticking the boxes, but not appreciating the challenges that change presents.

The 2013 APSC Review of ABS capability assessed whether ABS's people, systems and processes were aligned to current objectives and future challenges. The Review's findings provide insights into ABS culture at that time, including:

- The ABS has clear vision with a strong future focus, which is well communicated and understood by stakeholders and staff at all levels.
- The ABS views itself as independent and highly capable in its field. The ABS has a strong reputation as a respected and trusted institution and a professional and motivated workforce with a 'deliver or die' mentality.
- The manner in which the ABS has exercised its independence has contributed to organisational isolation and insularity. ABS staff tend to

have longer than average tenure, which builds deep expertise, but further contributes to an insular, inward-looking culture.

- The ABS had problems locating itself in government. Its connections with central agencies are inadequate. Stakeholders have limited involvement in developing policy and strategy, and relationships needed to be more open and collaborative, rather than ABS-centric.

The APSC concluded that transformation of ABS capability was needed in all aspects of the capability framework —leadership, strategy and delivery. It requires that deeply-held ABS values and culture be tested against the changing policy and information environment and refreshed where needed.

Also insightful of ABS culture and capability are the findings of consultancy CapDA's review of 2016 Census ICT capacity and capability, finalised in May 2014. CapDA found deficiencies in ABS capabilities such as project management, architectural governance and software development practices, including that:

- Although the ABS has project management expertise, rigorous project management is not strongly embedded within the culture and behaviours of the ABS.
- The way the ABS uses agile software development method means that dealing with security, high performance and accessibility are considered late in the cycle.
- It was unclear where, and in whom, the responsibility and authority is vested for making key architectural decisions.
- There was no evidence that any application or data centre performance monitoring is in place.

Subsequent reviews confirm some worrisome traits persist.

One such review, in June 2016 (an ABS-initiated review of stakeholder relationship health), reported stakeholders saying that:

- The ABS is not driving strategy and new developments are led by other, more proactive agencies who better understand the opportunities and possibilities for reform.
- The ABS's business model is old, outdated and in need of renewal.
- The ABS is almost missing the potential of the digital age by clinging to past practice.

But the Reviews conducted in the past two years also attest that the ABS is taking meaningful action to bring about much-needed change.

A complex environment for the ABS

It would be remiss to not acknowledge that the preparations for the 2016 Census took place during a challenging time for the ABS. The early stages for the preparation were led by the former Australian Statistician Brian Pink who retired in January 2014. Mr Pink appeared intent on leveraging the Census to

enhance the 'rest of ABS's capability because investment in refreshing the ABS's aging and fragile infrastructure was not forthcoming.

During most of 2014 the ABS had an Acting Australian Statistician and there was considerable uncertainty about the substantive filling of the position. David Kalisch was appointed as Australian Statistician in December 2014.

The cultural change journey continues…

The ABS has devoted energy and resources to aggressively address the cultural issues highlighted in the APSC Capability Review.

In May 2015 the Government announced an investment of $257 million over five years to modernise infrastructure, systems and processes used to produce critical statistics. This is the largest infrastructure investment in the ABS in the ABS's 110 year history. The investment will maintain the integrity of the ABS's core services, and ensure it is well positioned to meet the information needs of today's dynamic economy and changing environment.

Alongside this statistical infrastructure refresh, the ABS is progressing a broader whole of agency transformation that is focused on improving its key stakeholder relationships, concentrating on its key priorities, modernising its governance, having a more diverse workforce and improving its organisational culture.

Initiatives under Mr Kalisch include:

- The ABS's leadership group made, as an ongoing priority, communication with staff that emphasises the need for change, a new vision for the future; and the comprehensive approach required to achieve the necessary outcomes.
    - A 2016 staff survey found that 80 per cent of ABS APS staff had a good understanding of the broad transformation vision and goals and were motivated by them.
- The ABS has been restructured to better align organisational structure and priorities, including by creating new divisions with a focus on stakeholder engagement and organisation transformational-change.
- The ABS is part way through a process to modernise the way it engages with risk. In time, this will be rolled out across all statistical areas, including the Census area.
    - New risk management framework and guidelines are being developed and implemented, starting with the main economic indicators, and in turn confronted by independent external audit.
    - A Statistical Strategy Committee was formed at the end of 2015 to provide advice on the ABS statistical work program, with a key focus area being statistical risk.
- The ABS has placed greater priority on stakeholder engagement, including developing and implementing an engagement strategy, following consultation with stakeholders.
    - Relationship management has been embedded as a core part of

ABS business, with clear accountabilities established for building and managing relationships with key stakeholders.

- Regular stakeholder reviews are conducted to measure progress and to adjust strategy e.g., Briggs Health Assessment.

In 2016, the ABS is trying hard to transform itself in response to previous reviews. It has made progress. For example, the Brigg's Health Assessment found that:

> "Almost three-quarters of stakeholders have experienced improvements in the ABS's engagement with them since the capability review was conducted in late 2013."

But the ABS still has some way to go to achieve its transformational goals.

Culture and the eCensus – selected case studies

"a culture of building and operating complex purpose-built systems in preference to standardised, automated and common user systems and tools" – ABS 2017 Program Plan, June 2012

A few examples illustrate how ABS culture affected decisions and performance as the ABS planned and carried out the eCensus. These examples highlight behaviours that were exposed by earlier reviews.

Going it alone: The ABS's false start to the 2016 eCensus

The ABS decided, as part of its ABS 2017 transformation programme, not only to consolidate all its corporate electronic forms solutions into one system, but also to use that solution for Census 2016.

The ABS determined that *Expression of Interest* responses from the market, including from IBM, did not add advantage over its own solutions. The ABS's preference was a Netherlands government-owned science and statistics product, called Blaise, which could also be used to conduct surveys.

Using Blaise, the ABS attempted to build its own online form for the 2016 Census, fuelled by good ICT architectural intent.

After extensive development and testing, however, the endeavour ultimately failed to meet eCensus performance requirements. In particular, Blaise could not be architected to scale to eCensus volumes.

The CapDA May 2014 review into ABS Census 2016 ICT capability, commissioned after the failure of Blaise to meet Census 2016 requirements, found deficiencies in ABS capabilities such as project management, architectural governance and software development practices.

Reflected in this lengthy, aborted, effort are traits deep seated in the ABS at the time. Viewing itself as independent and highly capable in its field, and seeing the Blaise eCensus solution as part of a complex transformation programme, the ABS felt confident enough to compare its own efforts against market offerings.

This attitude illustrates the ABS's tendency at the time to look inward for future solutions and shows that the ABS was overly confident in its own abilities. It

showed little recognition of the need to acquire significantly different skills for digital first service delivery.

Hand in hand: The ABS and IBM

The ABS 2017 Transformation Steering Committee learned in November 2014 that the ABS's internal-forms capability was unable to support Census electronic form volumes for 2016. The Steering Committee was asked to endorse the agreed fall-back position, which relied on the old IBM eCensus instrument used for the 2006 and the 2011 Censuses. The fall-back position to the old IBM 2011 solution had already been agreed in May 2013.

The May 2014 CapDA consultant's report noted that an open tender would normally be the option most likely to provide ABS and the taxpayer with the best combination of value for money, innovation and risk mitigation. However, the report recommended that the ABS seriously consider a limited tender to IBM to reduce the risk of an already high-risk program.

On 20 June 2014, the ABS CIO approved the procurement plan for a limited tender to be issued to IBM for an eCensus solution (online electronic form). Once IBM was given responsibility for delivery, the key architectural decision to host the 2016 Census online form in a fully dedicated facility followed. Other alternatives were considered and rejected as part of that architectural decision, including the alternative of primarily using cloud infrastructure.

Project documentation shows that the ABS knew (and was more than likely substantially comforted by the knowledge) that it could use the successful 2011 online Census solution (eCensus) in 2016 if its own efforts failed.

Still burdened with the characteristics and cultural traits that it is now working hard to change – insular, not forward-looking, deficient risk management – the ABS locked itself in with a trusted partner.

Together the ABS and IBM were now committed to basing the 2016 online Census form on a solution that had its origins in 2006. The ABS had, in effect, denied itself the opportunity to leverage conditions and capabilities that were changing rapidly over the decade.

Hello again: The communications campaign

The ABS's plan for its communications campaign leading up to the 2016 Census appears to have been based on two questions: What did we do last time? Did it work?

The answers were clear. The 2011 Census campaign had focussed on raising awareness of the Census and of its utility. And the campaign had been successful – indeed, award-winning.

2016's campaign, then, was to be much like 2011's.

But, the world of communications had changed, and so had the government's commitment to online activity. That increasing amount of government activity online was causing public concern with privacy and with security of data. And

the rise of social media gave those with such concerns an ever-stronger platform to spread their views.

Raising awareness of the Census was not the problem in 2016. But that is where the ABS put its efforts, leaving a vacuum in the public debate and itself flat-footed when, in the final weeks before the Census, privacy concerns began to create a negative aura around the Census.

All's well: Assurances provided to Government

Leading up to the Census, in September 2015, the ABS reassured the Hon Alex Hawke MP, the new Assistant Minister to the Treasurer, that plans for the Census were in hand.

> "Preparations for the Australian Census commenced over three years ago, and the new approach has been tested multiple times through public tests. A major test of 100,000 households conducted in August 2014 confirmed our strategy and capability for the 2016 Census."

In the following months, the Assistant Minister's Office sought detailed briefing on the Census, including: privacy, digital capacity and the major risk mitigations in place for the Census. On 25 February 2016, the ABS emailed a brief to the Minister's Office on the online form's resilience, of which excerpts state:

> The ABS, in partnership with IBM, has gone to significant lengths to ensure the best possible experience for users, with key considerations being availability, speed, usability, access from different devices, reliability and security.
>
> ABS and IBM partnered together to deliver highly successful online forms for the Census of Population and Housing in 2006 and 2011, which received forms from 10 per cent and 33 per cent of the population respectively. The preparations for 2016 leverage this experience and investment, as well as incorporating further advancements to take advantage of emerging technology.
>
> The 2016 Online Form is based on the proven application and infrastructure design that was successfully used in previous Censuses, and like previous Censuses will be hosted from IBM's data centre in Baulkham Hills, Sydney.
>
> ABS, IBM and Government security experts collaborate to ensure the robustness of the Online Form, including monitoring the external environment for security threats to the Form like Denial of Service and hacking attacks.
>
> The Online Form infrastructure is architected to ensure that all components have complete redundancy so that hardware failures do not cause any reduction in service or service outages.
>
> The solution is rigorously tested by both IBM and by ABS-appointed independent companies to ensure that it has the capacity, resilience and security to deliver the required service levels.

Similarly, in mid-2016, the ABS gave assurances to the Hon Michael McCormack

MP, the new Minister for Small Business, and the Minister responsible for the ABS, that all was well with the Census:

> "The ABS is confident that it will deliver another high quality Census."

The briefings provided strong assurances of the effectiveness of the ABS systems and procedures. The ABS made clear its confidence in the reliability and security of its systems, conveying assurances to government that the Census would be successful.

The briefings showed the ABS demonstrating over-confidence in its abilities and conveying its own sense of comfort in the proven technology that it was deploying.

The briefings did not recognise the implausibility of guaranteeing complete success in an online landscape. Nor did the briefings display any ABS acknowledgement of the whole-of-government aspects and ramifications of the eCensus.

Looking backward

The ABS culture clearly contributed to the outcomes on Census Night. The ABS actions since only underscores the importance of culture: while it has said 'sorry' on a number of occasions it has steadfastly refused to own the issue and acknowledge responsibility for the factors leading to the events and shortcomings of events on the night:

- it repeatedly cited evidence that the Census response rates are on track so there is no problem;
- it has ignored public sentiment, particularly on social media, following the incident; and
- its public submission to the Senate Inquiry laid clear blame on IBM without acknowledging their own contribution.

Looking forward

Preparations for the 2016 Census were in train since 2012. Many decisions were taken ahead of the recent reviews and the significant investment the ABS has made in the transformation of its organisational culture.

As a result, cultural insights from the 2016 Census at least partly reflect the old culture: the ABS has started on the journey to transformation and progress is clearly evident.

Nevertheless, the Census incident is a reminder that the ABS will remain exposed and its effectiveness compromised the longer it takes to achieve its goals to transform its organisational culture.

A key risk is that the ABS doesn't drive deeply enough into the organisation and instead attempts to achieve cultural change through a discrete set of technical responses, rather than as an integrated strategy.

In this regard, the Briggs stakeholder health assessment finds in relation to initiatives to improve stakeholder engagement:

> All stakeholders said that improvement to date was just the beginning of what needs to be done, and that there is no room for complacency.
>
> Stakeholders have concerns that changes at the top are not being mirrored by those further down in the middle and senior executive service ranks of the organisation.

Recommendation:

The ABS should draw upon the lessons it takes from the Census experience to help to guide and to advocate for the cultural change path it is following.

2.6 Contractual Obligations

Key findings

- Evidence on the question of contractual compliance indicates a failure by IBM, through its own actions, and the actions of its suppliers, to provide adequate DDoS protection.

IBM had a contractual obligation to ensure that the hosted eCensus environment was protected from DDoS attacks. The available evidence indicates multiple failures and a range of deficiencies in the implementation of the recommended DDoS attack-protection strategies by IBM and its suppliers.

There are two key contractual issues to be considered in relation to the events of 9 August:

1. understanding the contractual obligations in place in relation to DDoS; and
2. establishing whether or not those obligations were complied with.

Evidence as to the first issue is clear. IBM had an explicit and acknowledged contractual obligation to ensure that the hosted environment was protected from DDoS attacks, particularly during the peak Census period. There is no evidence that the ABS ever released IBM from this obligation or varied it in any way.

Evidence on the question of contractual compliance indicates a failure by IBM, through its own actions, and the actions of its suppliers, to provide adequate DDoS protection. IBM may dispute some details of the alleged failings, for example whether or not the false warning as to data egress justified the closure decision, but it is clear that there was a failure of implementation in relation to DDoS protection, a matter for which IBM was contractually responsible.

What contractual obligations were in place in relation to DDoS attacks?

Contract documents

In July 2014 the ABS issued the *Statement of Requirements for the 2016 eCensus Solution ABS2014.105*, containing details of the eCensus Solution (the eCensus Application and the eCensus Hosted Environment) to be provided by the selected Prime Partner.

Under the heading 'Security', the *Statement of Requirements* included the following statement relating to DDoS:

> *The Application must be built to current industry best practice to prevent attack against the Application, hosting infrastructure or respondent's computer. The hosted environment must be protected from Distributed Denial of Service (DDoS) attacks, particularly during the peak collection period.*

Simultaneously the ABS issued a *Request for Tender for eForms Solution ABS2015.105* (RFT), published on 25 July 2014. The RFT attached the *Statement of Requirements* and tenderers were required to address their ability to comply, including providing detail of proposed DDoS protection and mitigation measures.

On 22 August 2014, IBM submitted a compliant tender response which included a section dealing with prevention of attacks and protection from DDoS during the peak collection period.

In its response, IBM described a range of proposed security controls and specific measures to provide protection from DDoS including:

- ability to block IP addresses and ranges at the entry firewall and the entry router;
- ability to block source IP addresses and ranges at the BGP Gateway, and at the ISP end of the BGP link through negotiation and tools provided by the ISP vendor;
- a negotiated agreement to block all international access to the eCensus Solution when requested; and
- engagement of a DDoS mitigation service from an external provider (NextGen).

The *Statement of Requirements* and the IBM tender response of 22 August 2014 were incorporated into a contract between the Commonwealth of Australia, represented by the ABS, and IBM Australia Limited for *Services for eCensus and Data Capture Solutions ABS2014.105* (contract). The contract was executed on 30 September 2014.

Service Level Agreement

Attachment 4 to Appendix 1 of the Contract, *Specific Requirements for Managed Services*, sets out details of the required hosting environment requirements and the 2016 *eCensus* Service Level Agreement setting out further details of IBM's responsibilities and required levels of service. This Attachment includes confirmation that:

> *…[IBM] is responsible for the development, delivery, implementation and hosting of the eCensus system, including the eCensus Application, in accordance with the criteria and timeline established by [the ABS].*

The Service Legal Agreement also includes requirements that:

- during the period 7pm to 11pm AEST on Census Night, the *eCensus* must be available for 98 per cent of this period; and
- from 7pm to 11pm AEST on Census Night, any fault is to be categorised as critical and has a maximum time for fault resolution of 30 minutes.

Events after September 2014 in relation to DDoS protection strategies

Discussion as to the detail of IBM's DDoS solution and the implementation of

that strategy, the 'Island Australia' strategy is detailed elsewhere in this report. At no stage did IBM seek to resile from its obligation to provide DDoS protection. At various times, assurance was sought from and provided by IBM that its recommended DDoS strategy was sound and effective. For example, the DDoS strategy was discussed by the project Risk Management Committee at the Risk Management workshops and was included in various project Risk Management Plans.

Additionally, testing of the 'Island Australia' Strategy was conducted on 5 August 2016 and advice provided by IBM that the testing had 'worked as expected'.

There is no indication of any step taken by the ABS to release or waive IBM from its responsibilities relating to DDoS. To the contrary, the material reviewed indicates a continuous reliance by the ABS on advice provided by IBM that an appropriate strategy for DDoS protection was in place and that agreed mitigation measures would be implemented.

Summary of legal obligations

The contractual framework established in September 2014 includes a clear legal obligation requiring IBM to take such steps as were necessary to mitigate DDoS attacks, particularly during the peak period, and to ensure the minimum availability requirements and fault resolution timeframes were complied with.

Did IBM comply with its contractual obligations in relation to DDoS attacks?

IBM had a contractual obligation to put in place measures sufficient to protect the hosted eCensus environment from DDoS attacks, particularly during the peak Census period. It is clear that IBM was unable to mitigate DDoS attacks. While it is understood that in some instances even the implementation of protection in accordance with current industry best practice does not guarantee that a DDoS attack will not bring down or adversely affect a website, the evidence in this case indicates that IBM failed to implement adequate DDoS attack mitigation measures. The reasons for the failure appear to be multiple and involve a range of deficiencies. These include:

a. a failure by IBM to instruct or communicate with its subcontractor ISP, (NextGen Group) and upstream providers (Vocus) in relation to the requirements of the agreed DDoS attack mitigation strategy 'Island Australia';
b. a failure by IBM to supervise or ensure the proper performance by NextGen Group or upstream ISPs in relation to the implementation of the agreed DDoS attack mitigation strategy 'Island Australia';
c. a failure by IBM to configure the router at the IBM end of the Telstra link so that it would reload its configuration upon rebooting;
d. a failure by IBM to test the settings in the router at the IBM end of the Telstra link to ensure proper performance;
e. a failure by IBM to conduct adequate testing of its recommended 'Island Australia' DDoS attack mitigation strategy;
f. a failure by IBM to recognise or read or interpret signals correctly leading to a false alarm of a spike in outgoing data and the

possibility of data egress;

g. failure to implement or configure the network performance monitoring system(s) such that they incorrectly provided, and were unable to validate, an indication of data egress;
h. failure to set an appropriate session time out value for the HTTP worker threads on the web servers; and
i. a failure by IBM to recommend to the ABS a suitable default or redundancy strategy in the event of failure of the recommended 'Island Australia' strategy.

It was IBM's responsibility, as the party engaged to provide the services, to ensure that the recommended and agreed protection strategy was effectively implemented. This responsibility required that IBM provide adequate instruction and direction to those parties whose services formed part of the overall response strategy for which it was responsible.

One area which IBM may dispute is the 'false alarm' relating to the possibility of outgoing data. The issue of the 'false alarm' is significant because it was *the key factor in the decision to close the eCensus form, and in the site remaining down until it could be established that no Census data had been compromised. Other factors contributed to this decision point, but the ABS's decision to close the eCensus form was made on concern that Census data was being compromised, based on this single indication, under the circumstances of a broader attack*. The notification of unexpected outbound traffic occurred at 19:45 on 9 August and it was not until around 2:00am on 10 August that IBM was able to advise ASD that the notification was a 'false positive'.

The failure by IBM to provide accurate advice on the traffic spike of outbound traffic suggests a lack of preparation or diligence in monitoring. IBM may not accept this view.

In summary, however, there is evidence of failings in three broad categories by IBM which indicate it did not comply with its obligations relating to DDoS protection:

1. Failings relating to the non-implementation of 'Island Australia' by IBM's sub-contractor NextGen Group and its upstream providers – including failures by IBM to ensure the agreed strategy was properly activated or tested.
2. Failings relating to configuration of the router at the IBM end of the Telstra link.
3. Failings relating to the 'false alarm' and an inability to provide accurate advice in relation to the outbound traffic spike.

PART 3: INTEGRITY OF THE CENSUS

Key findings

- eCensus outages saw many Australians put off completing their Census forms. This reaction initially reduced response rates. It also saw more Australians turn to paper forms.
- The ABS had 38,000 field staff visiting households yet-to-complete their Census. It adjusted the pattern of these visits to mitigate the impact of outages on household response rates.
- The Census response rate, a critical indicator of quality, is estimated to be over 96 per cent. At this stage, it is unclear if the target rate of 96.5 per cent will be met. This target is based on the rate achieved in the 2011 Census.
- A more granular assessment of Census quality will not be available until data has been processed, expected completion in March 2017. A preliminary assessment will be possible in October 2016.
- Current indications are that other quality indicators such as refusals and item non-response rates are likely to be comparable to, or better than, outcomes in the 2011 Census.
- Unaware of these encouraging signs, post-Census surveys find that many Australians believe that the data collected is unreliable. A targeted communication strategy will be critical to addressing these perceptions.

Recommendations:

- The ABS's decision in August to assemble an independent panel to provide assurance and transparency of Census quality is supported and the resulting report should be made public.
- The ABS should implement a targeted communication strategy to address public perceptions about Census data quality.

Why is it important to have a high-quality Census?

The Census produces statistics that underpin critical decisions by governments, business and the community

The Census is the official count of population and dwellings in Australia and also collects details of age, sex and other characteristics of the population. It is the ABS's most widely used and most referenced data set.

The Census' primary aim is to measure the number of people in Australia on Census Night, along with their demographic and geographic characteristics.

The Census is the primary source of regional and small-area statistics. It is also the richest source of data for small-population characteristics, containing detail regarding occupation, industry, education and diversity.

The Census is used to determine the number of electoral seats for each State and Territory, to support electoral boundary re-distribution, and to allocate Australian government funds to state, territory and local governments.

Furthermore, Census data also supports the planning, administration and policy-development activities of governments, business and other users, for example, infrastructure planning and service delivery.

How can we assess whether the Census is fit for purpose?

Four main types of potential error can occur in Census data, each important to an assessment of whether the Census is fit-for-purpose. These are:

- **framework error** — error due to inaccuracies in the Census address register that are not subsequently resolved;
- **non-response error across dwellings, persons and data item** — error due to incomplete data at the dwelling, person and data item level;
- **measurement error** — error due to incorrect answers to questions, both intentional and unintentional; and
- **processing error** — error due to coding of paper forms.

The eCensus outages are most likely to have impacted non-response error as the outages apparently caused many Australians to put aside their Census form and not get around to completing it online. The follow-up by the ABS, outlined in the next section, aimed to mitigate this problem.

The most critical type of error to manage in the Census is non-response. Higher levels of non-response error can lead to higher levels of error in the estimated population, which reduces the quality of the Census. Managing the uniformity of the distribution of non-response error across small-area and population groups is particularly important, as the Census is the key source of statistics for these groups.

No objective standard exists for an acceptable level of non-response error in any Census. Some non-response is inevitable; the question is what rate of non-response is low enough to assure the Census is of good quality.

Ahead of the 2016 Census, the ABS set targets for non-response error that broadly sought to equal or outperform 2011 Census outcomes and those in other countries such as the United Kingdom. The ABS had mitigation strategies in place to achieve these targets, strategies outlined in the next section.

Against the benchmark of the 2011 Census, a credible test of whether the 2016 Census statistics are fit-for-purpose is:

(1) **Census response rate** of 96.5 per cent of occupied dwellings, which is the level achieved in the 2011 Census;
(2) **Uniformity of the distribution of Census response rates** across designated **statistical areas** of 100,000 persons and **population groups** (e.g., indigenous, young adults) that is superior to the 2011 Census;
(3) **Census item non-response rate** equal to, or less than, the 2011 Census for key Census items, including name, which is important to minimise the Census undercount; and
(4) **Census undercount** of 2 per cent (see Box 3). This rate is higher than the undercount of 1.7 per cent in the 2011 Census, but is justified given the increasing mobility of the Australian population. It is less than that achieved for the 2006 Census (see Box 3).

In relation to other types of error, the following metrics could be added to an

assessment of whether the 2016 Census statistics are fit-for-purpose:

(5) **Frame error.** A reasonable test is whether the percentage of unresolved addresses is less than 0.5 per cent.

(6) **Measurement error.** The ABS will publish an evaluation of the quality of each item, as it did for the 2011 Census. This evaluation will be based on factors, such as item non-response rates, the percentage of records with insufficient information to code accurately, and the validity of comparisons with the 2011 Census and other statistics.

Finally, it is necessary to understand public perceptions of the Census as users of the statistics, and the public more generally, must see the Census as credible. This credibility is to ensure that Census statistics are used for their intended purpose and that the public provides quality responses to future Censuses.

(7) **Credibility of Census statistics:** the percentage of the population who believe the Census data are reliable. The ABS is collecting this information. A significant reduction in public perceptions of poor quality should be observed before the Census data are published. This is likely to require a targeted communication strategy.

Box 3: Estimating the resident population in Australia

A measure of the undercount in the Census is obtained from a short sample-survey of 50,000 households undertaken shortly after the Census, called the Post Enumeration Survey (PES). This Survey collects information about where people were on Census Night and their characteristics, which are compared to the actual Census forms.

From the matched records, it is possible to estimate the net undercount, that is, an estimate of how many persons were missing on Census night. The accuracy of this process will depend on the quality of the PES, especially the response rate.

Where information is available for non-responding households, Census details are imputed, especially for key characteristics, such as age or sex. This information will be less accurate than for those households where data were actually collected.

As a result of the imputation, the Census undercount will normally be less than the non-response rate. For example, the non-response rate for the 2011 Census was nearly 4 per cent, but the undercount was 1.7 per cent.

Meeting these eight metrics is not a guarantee that the outages have not had an impact on Census quality. Instead, the assessment will judge whether that impact was small, including as a result of the mitigation strategies.

On the other hand, if the data fall just short of these metrics, the Census may still be fit-for-purpose. The assessment is likely to be that the Census is still fit-for-purpose, although of somewhat lower quality than planned and the 2011 Census.

In the event that these metrics are not met by a considerable margin, the

usefulness of the Census will be under question.

What mitigation strategies did the ABS have in place to optimise Census quality?

Every Census has some error. In particular, every Census has some under-reporting of dwellings, persons and data items.

Quality management of the Census program aims to reduce error as much as possible, and to provide a measure of the remaining error to data users, allowing them to use the data in an informed way.

Strategies to optimise Census quality were built into all stages of the preparation of the Census, and their effectiveness will be reflective in the first seven metrics mentioned above. Although largely eliminating errors during the preparation phase is highly preferable, the Census also has in place a set of quality-assurance processes that are applied during the processing phase.

The main strategy to address under-reporting of dwellings is the 38,000 Census field staff who visit households yet-to-complete their Census to solicit responses.

In the 2016 Census, the ABS used an adaptive-design approach to the Census field work: non-responding dwellings were grouped together post-Census into logical workloads and allocated to Census field staff.

This adaptive-design approach allows the ABS to monitor response patterns at a local level and to make quick adjustments to field staff workloads in response to these patterns. This adaptability targets resources to achieve higher uniform response rates across Census sub-groups.

In addition to these approaches, about 30 per cent of geographical areas were pre-identified as requiring a different approach. In these areas, field visits commenced directly after Census night to target low-compliance or transient populations more quickly. Specific strategies from previous Censuses have also been enhanced for enumerating hard-to-reach segments of the population, such as remote indigenous communities and rough sleepers.

The ABS's strategies are likely to have enabled an appropriate response to the impact of the Census outage on the number of responding dwellings, particularly if there was some geographic differentiation in the impact. It would also be expected to assist in addressing hard-core refusals, as face-to-face contact with Census field staff can help to persuade those refusals to co-operate. However, none of these strategies will completely mitigate impact on non-response by item, although the early analysis in **Table 1, page 80**, is promising.

What is the impact of system outages on Census data quality?

Once Census data has been processed, it will be possible to rate the 2016 Census against the proposed benchmarks that jointly assess whether it is

fit-for-purpose. Data processing is expected to be completed by March 2017. However, isolating the impact of outages on Census data quality will be difficult.

At this stage, the high level of public co-operation suggests that although the outages led to significant negative publicity, they may have increased awareness of the Census and not have had much impact on response rates.

It is worth noting that the 2016 Census eform rate is much greater than that of the 2011 Census and this higher rate will likely improve Census quality: the evidence from the 2011 Census was that eforms were of higher quality than paper forms.

58 per cent of households participated online, compared with 33 per cent for the 2011 Census.

Non-response Error

The Census outages prevented Australians from filling in forms online for 43 hours. This not only precluded online responses during the outages, but also likely reduced online responses over subsequent days due to confusion about security and the status of the eCensus. Considerable catch up then followed.

Ahead of the Census, the ABS conducted a series of tests that suggested that 65 per cent of households would participate online (5.6 million) and 35 per cent would respond using paper forms (3.0 million).

Against this benchmark, response-rate data suggest that more Australians than expected decided to use paper forms following the outages (see Figure 6).

As at 10 October, the Census response rate is estimated to be over 96 per cent, broadly in line with the planned target response rate (see Figure 6).

- Estimated response rates will likely rise during the processing phase, as individual responses are analysed more closely, such as whether non--responses are due to dwellings being unoccupied on Census night

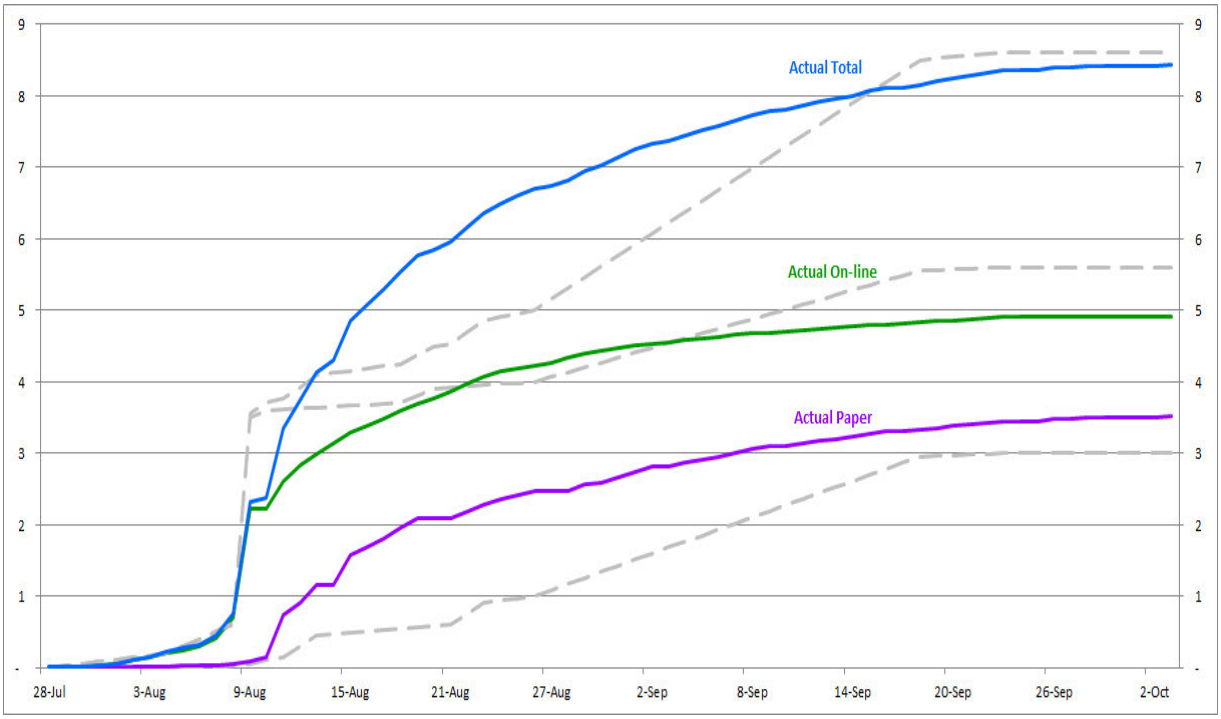


Figure 6: 2016 Census Response Rates (as at 2 October 2016)

Whether hard-core refusals will increase compared with previous Censuses is not yet clear. At 20 September, the number of refusals was low at 6,743, compared with 13,194 in 2011. The number of refusals is likely to grow, but remain smaller than in 2011.

Meaningful estimates are available for item non-response rates - see **Table 1** (Benchmark 3). At this stage, estimated rates are lower than 2011 Census outcomes (except for name, where data are not available). The higher proportion of more accurate online forms would have helped in this respect.

Item	2011 Census (per cent)	2016 Census (per cent)
Name (2)	N/A	1.2
Age	0.5	0.4
Country of Birth (3)	2.1	2.6
Indigenous Status	1.5	0.8
Australian Citizenship	2.3	1.6
Income	4.2	3.2
Student Status	2.8	1.7
Religion (4)	5.0	4.0

Table 1: Estimated item non-response rates: Selected items (1)

(1). The weighting used in the estimates assumes 60 per cent of forms will be received online and 40 per cent will be received on paper.
(2). Not compiled for the 2011 Census.
(3). The 2011 Census includes responses derived from other information on the Census form. This process has not yet taken place for the 2016 Census.
(4). A voluntary question.

Estimated item non-response rates are based upon submitted online forms and the paper forms scanned to date. The sample of paper forms may not be representative of all paper-form responses, as the more co-operative

respondents will tend to respond (and be scanned) earlier. Therefore, it is too early to say that the item non-response rates for the 2016 Census will be lower than for the 2011 Census, but there is reasonable confidence that they will be at least comparable.

Data to assess whether benchmarks are met for distribution across population groups and geographical areas (Benchmark 2), for item (Benchmark 3), and for undercount (Benchmark 4) will not be available until mid-2017. The ABS plans to put this information in the public domain, which is important for informed use of Census data.

Framework, measurement and processing error

Every Census has a single reference night, but not every household completes the Census on this night; inevitably the collection period extends over some weeks.

The delays in the response of the mainstream population due to system outages are unlikely to lead to significant recall error (i.e., measurement error). Most data items collected in the Census, except possibly location on Census night, do not change quickly. Even if some recall error exists here, the Census statistics are compiled on 'usual residence' basis, and most households can recall accurately where they usually lived.

On the other hand, collecting information for more transient groups of the population very close to the Census night (e.g. travelers, homeless, and hospital patients) is important. Collecting data from these groups does not rely on the online form and so should be largely unaffected by the outages.

Security and privacy concerns due to the data-retention policy and the Census outages may have led some Australians to misreport data deliberately. More likely, people with these concerns would simply not answer certain questions. This attitude would be reflected in the item non-response rate.

Data to assess whether system outages have impacted on the quality of the data supplied by households will not be available until processing is complete. However, early analysis of item non-response rates provides some confidence that any impacts will be minor. A sample check of the online forms suggests very few have not put in a name or have used a fake name (1.2 per cent – see **Table 1**).

Data to assess whether the benchmarks for framework and processing error are met will not be available until the end of 2016 and April 2017 respectively.

How can the ABS maintain public confidence in Census quality?

On Census night, and in the subsequent outage period, system failure and the slow and inadequate communication with the public caused confusion, contributed to concerns about data security and reduced public confidence in the Census. The actual impact on data quality is uncertain, but the outages have raised public concerns about Census quality.

The ABS conducted surveys of public attitudes towards the 2016 Census in the aftermath of the Census. The surveys found that many respondents believed

that the data collected would be unreliable. In particular, the latest Survey found that:

- **42 per cent agreed, to some extent, that this year's Census has been a failure; and**
- **33 per cent agreed, to some extent, that the data collected from this year's Census are unreliable.**

For the Census to be fit-for-purpose, the users of the statistics, and the public more generally, need to see the Census as credible. This credibility is to ensure that Census statistics are used for their intended purpose and that the public continues to provide quality responses to future Censuses.

Given the public concerns about the quality of Census outputs, the ABS has proposed that an independent panel be assembled to provide assurance and transparency of Census quality.

This Review strongly supports the ABS's establishment of an independent panel and suggests that the panel review the metrics as soon as suitable data becomes available. The panel should review, and if appropriate adopt and supplement, the benchmarks that are outlined earlier in this Review.

This Review proposes that the resulting report is published. This openness will be important for public assurances that Census data are fit-for-purpose (should this be the case).

Recommendation:

The ABS's decision in August to assemble an independent panel to provide assurance and transparency of Census quality is supported and the resulting report should be made public.

The current perception, even among many well-informed users, is that Census quality will be significantly affected by the outage. There will need to be a carefully targeted communication strategy to address this perception. It should be aimed at the public and opinion leaders as well as key users.

Recommendation:

The ABS should implement a targeted communication strategy to address public perceptions about Census data quality.

PART 4: CONFIDENCE IN A DIGITAL FUTURE

Key findings

- A transition to digital is inevitable and increasingly citizen driven.
- Much of government does not yet understand how to embrace and exploit digital.
- Maturing government's approach to digital will require mindset shifts and capability uplifts, as well as adapting frameworks and practices to new ways of working with technology.
- Digital technologies can help government to lower project costs and risks, and will provide opportunities to increase government transparency and citizen involvement.

Recommendations

- **Cyber Security in a Digital First World:** The Digital Transformation Agency, in partnership with the Australian Signals Directorate and the Department of Finance, should:
    - develop a proposal for consideration by the Digital Transformation Committee of Cabinet to create a "cyber security shared services" digital security consulting organisation within the Digital Transformation Agency. This would ensure security is integral to all new online service delivery proposals and facilitate partnering between agencies to draw on cyber security expertise in larger agencies with more mature capabilities.
    - consider how to strengthen central governance and assurance, and this ownership may no longer logically sit with ASD, given their broader portfolio of responsibilities.
    - identify capable agencies and accredit them to deliver shared services for citizen-facing projects where, for higher risk online delivery programs, smaller agencies must partner with (or source their ICT project management from) an identified lead agency or through a core service such as GovCMS.
- **Creating a Positive Risk Culture:** The Department of Finance should assist agencies to actively engage with cyber security risk by developing a strategy to accelerate government to improve agency understanding and uptake of secure cloud services and hasten cloud certification to PROTECTED (potentially modelled on the US FedRAMP program). This would require additional resources for the Australian Signals Directorate for accreditation services. The Australian Signals Directorate should come back to government with a plan coordinated with the Cyber Security Special Adviser.

Transition to digital engagement is inevitable and citizen driven

Government digital service delivery should be:

Consistent and simple to use...

Focused on the user, not the structures of government...

The eCensus adds to a roll call of suboptimal government online outcomes – myGov, Auskey, the National Disability Insurance Agency and e-health records – suggesting that government capacity to deliver digital services is failing.

Citizens are, however, increasingly requesting and consuming services digitally in all areas of their life and government services cannot be exempt or different.

Many aspects of people's lives have now migrated online. The digital economy provides groceries, clothing and taxis. The social web is how friends are updated, memories shared, partners met, travel booked, restaurants recommended, music streamed and TV watched. At a household level it is how finances are managed, and bills paid.

Available at any time, on any device, and inclusive for disabilities…

Secure and private…

…but with data sharing where appropriate

The ABS's decision to increase digital uptake of the Census correctly identified Australians' growing preference for the speed and convenience of online transactions over other channels. Despite the flawed execution and attendant negative publicity, electronic completion rates for the Census were around 58 per cent.

The early indications of public discontent with the Census and the real-time public dissection of the event via #CensusFail were also digital. This underscores the importance of online interactions in shaping public discourse and highlights the importance of government agencies understanding and managing the diverse digital channels that influence relationships between citizens and government.

Slow to embrace and exploit digital opportunity, let alone security

Government is not well equipped to understand new technology models and the ways of working that complement them

Technology models within government are still firmly rooted in data centre-based enterprise architectures rather than in the consumer technologies that are changing the way we live.

Government's ICT procurement processes have been developed over decades and are slow, cumbersome, expensive and increasingly inappropriate in the digital world. Business cases, financial governance, and contracting protocols evolved to support technology decisions that required heavy capital investment in infrastructure with a lifecycle frequently spanning decades. These processes create barriers to adopting, implementing and managing contemporary technologies because they emphasise long-term locked-in decisions and early stage certainty. As evidenced by the ABS-IBM relationship, these methods also leave government vulnerable to supplier lock-ins and obsolescence as the pace of technological change accelerates.

The digital economy offers faster, simpler and cheaper alternatives for service delivery that are best illustrated by consumer technologies such as Airbnb and Uber. These offerings are fluid, adaptive and often temporary. From a technical perspective, they can be stood up within months, and are then continuously developed in small, fast and inexpensive increments that are drawn from insights into user behaviours. Government has not traditionally looked to consumer technology models for its service design and lacks a coherent strategy to exploit their potential advantages.

GovCMS provides a common cloud platform used by 32 agencies to host 80 live sites

Consumer technologies can go to market quickly and cheaply thanks to the economics of public cloud platforms. Cloud computing can provide organisations with greater data storage capacity, cost savings, convenience and flexibility. The Government launched its Cloud Computing Policy in 2014, requiring agencies to adopt a 'cloud first' approach – where it is fit for purpose, provides adequate protection of data and delivers value for money. While there are potential risks associate with cloud, including loss of control of data and problems recovering data, with the right measures, cloud computing can be used in both the public and private sector to improve cyber security, particularly for small organisations.

However, with few exceptions (such as GovCMS), government digital services are not offered on the cloud. Most significant transactional solutions, including

"Agencies now must adopt cloud where it is fit for purpose, provides adequate protection of data and delivers value for money" (forward to Australian Government Cloud Computing Policy, October 2014)

myGov and myTax, are offered from physical, government-owned datacentres (sometimes referred to as 'private clouds'). These datacentres provide for re-use of shared infrastructure but do not benefit from the massive and instant scalability inherent in the distributed computing networks that comprise the public cloud. Government private clouds are significantly more costly than the public cloud because they are effectively competing on scale and efficiency with Amazon, Microsoft and others.

Following through on the intent of the 2014 'cloud-first' policy will demand genuine and sustained effort. The policy is strongly worded, but it lacks real measures by which cloud-first decision criteria can be judged or enforced and, in contrast with other jurisdictions, does not set any goals for its uptake.

The ABS displayed wariness in relation to data security and privacy in the cloud that is not uncommon in government. The agency appeared to be motivated more strongly by fear of non-compliance to privacy rules than by genuine misgivings about the protection of datasets. This mindset led the ABS to conclude that a public cloud solution could contravene its foundation *1905 Census & Statistics Act*, though the *Act* could never have contemplated the appropriate handling of data in the Digital Century. Unambiguous reassurance from a credible, central authority that cloud solutions are a preferred and legitimate option for government service delivery would go a long way to breaking down current barriers to adoption.

Recommendation:

The Department of Finance should assist agencies to actively engage with cyber security risk by developing a strategy to accelerate government to improve agency understanding and uptake of secure cloud services and hasten cloud certification to PROTECTED (potentially modelled on the US FedRAMP program). This would require additional resources for the Australian Signals Directorate for accreditation services. The Australian Signals Directorate should come back to government with a plan coordinated with the Cyber Security Special Adviser.

Mindsets, skillsets and frameworks all require overhaul. Traditional ways of working within procurement, project governance and risk management artefacts all fell short of ensuring an acceptable eCensus outcome. The ABS completed all the relevant procurement protocols, but still failed to address the specifics of the uncompetitive outsource in which it found itself. The ABS is, however, more common than an outlier in this regard. Traditional checklist-driven approaches to third party and program risk management do not provide adequate protection in a world of subtle risk and rapid change. The speed of change and the complexity of modern technology environments require context-sensitive decision-making and governance frameworks, and people who are skilled in their use.

Evident capability gaps affect the use of digital toolkits, including misinterpretation or misapplication of methodologies. The ABS had invested significantly in its own agile coaching and training, but to no avail. A flawed understanding of agile development led the ABS to delay scalability testing of its original Blaise Census solution until a late stage: "non-functional

requirements are not baked into the development lifecycle" (CapDA, November 2014). The delayed testing in turn led to the hurried appointment of IBM.

A number of agencies, including the ABS, produced draft digital transformation plans in early 2016. These point to digital capabilities that are often insufficiently mature to determine with confidence the most appropriate approach to a given digital challenge. Bespoke agile developments, off-the-shelf products and open-source collaborations can all be appropriate, but government buyers and technologists often lack the experience and decision frameworks to guide them to a successful selection, or to be a good digital customer for vendors once the selection has been made.

Cyber security: partnering for online services

Again, the experience of the ABS is not atypical. While some government agencies, such as the Australian Tax Office and the Department of Human Services, have robust and mature cyber security capabilities, the 2015 Cyber Security Review found that many agencies are struggling to keep up with constantly changing cyber threats. And many lack the necessary skills to implement security advice. The Review also found that it is difficult to assess the effectiveness of cyber security implementation across government as existing measurement tools largely rely on self-reporting and focus on compliance rather than the effectiveness of risk management strategies. More of the same is not enough: a new approach to helping agencies with cyber security is required.

The August 2015 review on 'Learning from Failure', by Professor Peter Shergold AC, called out the need for more adaptive government and enhanced responsibility and accountability for program management. In particular it recommended that agencies should actively source specific talent from outside the public service to provide a wide range of relevant skills, experience and entrepreneurial energy and to harness public service-wide expertise for managing high risk, large-scale projects.

There would be benefit in greater pooling of resources to help smaller agencies such as the ABS delivering citizen-facing services. Further, as the Digital Transformation Agency (DTA) enables more agile ICT development and delivery capabilities for government, cyber security must be 'baked in' to design and delivery. Phase Two of the Government's Digital Transformation Agenda offers an opportunity to develop a more "shared service" consultancy approach to cyber security to boost agency capacity and ensure ASD resources are focussed on high end cyber security risk.

Recommendation:

The Digital Transformation Agency, in partnership with the Australian Signals Directorate and the Department of Finance, should:

- **develop a proposal for consideration by the Digital Transformation Committee of Cabinet to create a "cyber security shared services" digital security consulting organisation within the Digital Transformation Agency. This would ensure security is integral to all new online service delivery proposals and facilitate partnering**

between agencies to draw on cyber security expertise in larger agencies with more mature capabilities.

- **identify capable agencies and accredit them to deliver shared services for citizen-facing projects where, for higher risk online delivery programs, smaller agencies must partner with (or source their ICT project management from) an identified lead agency or through a core service such as GovCMS.**

Building digital capability at all layers of government will create informed decision makers

Bridging the capability gap begins with creating awareness of the need for change at senior APS and ministerial levels. Government should consider introducing leaders from industry who are experienced in the digital journey, while also supporting skills acquisition in the APS through a Digital Academy similar to the UK's successful model. Synergies and common ways of working will arise from connecting digital communities together across agencies:

- **Build senior level awareness** of digital disruption possibilities through immersive study tours at Secretary and Deputy Secretary levels and within ministerial ranks. This approach was successful in accelerating private sector senior leadership commitment to digital.
- **Create quick capability uplift** by lateral hiring of private sector CDOs and the tier of specialists immediately below them, ensuring support for the cultural accommodations that both sides will need to make.
- **Build digital communities of practice** to encourage sharing and skills transfer between digital teams across government.
- **Support "Learning by Doing**" experiences that help agencies to create exemplars to kick-start their digital transformation.
- **Underpin with a Digital Academy** to empower motivated APS personnel to enhance their existing domain knowledge with digital skills.

Create whole-of-government approaches to digital service delivery to achieve scale economies

Significant financial and productivity benefits will flow from the creation of cloud-based 'building blocks' for common requirements such as payments and identity verification. These one-to-many digital platforms will reduce the delivery burden on smaller agencies; provide a trusted, assured baseline service to all; and decrease the unit cost of citizen servicing.

Digital platforms can be built using the resources of the DTA or using a lead agency approach. Both options will require significant cross-agency collaboration in gathering requirements for services that are common to many yet core to none. The most powerful incentive to collaboration is financial. Access to these platforms should be free of charge to agencies or close to it, and agencies that achieve a lower cost base through their use of common digital platforms should be rewarded in financial gain-share agreements.

Relationships with cloud services providers will need to accelerate and become

more sophisticated. Faced with low adoption of cloud services, the US government created the FedRAMP programme to standardise their approach to security assessment, authorisation and continuous monitoring for cloud products and services. The USA now has 69 certified providers, including 4 certified for "high-impact data, including data that involves the protection of life and financial ruin". Australia has only 4 certified cloud providers, all of whom can supply "unclassified DLM" environments such as that represented by eCensus. Australia has yet to contract for environments rated to PROTECTED – though this is under way. The government needs to offer a solution for PROTECTED environments in order for digital migration to be feasible across the government landscape.

Improve and formalise support and governance for digital programmes

The number and complexity of digital transformation efforts being planned or undertaken across government is increasing massively. With this increase comes greater potential for duplication of effort and for missed opportunities to create scale economies through the use of digital platforms. The potential also exists for the volume of overall activity to detract from delivering the most significant digital initiatives. Central accountability should be established to ensure that digital service transformations are efficiently structured and effectively delivered.

The mandate of this central unit should include coordinating, heat-mapping, and prioritising activity across all digital initiatives; maximising the use of reusable components and platforms; tracking progress and validating that milestones have been achieved in a staged funding model. It should also have a role to play in setting qualitative and quantitative benefits for initiatives and reporting against their achievement.

Smaller agencies such the ABS need better support for their digital transformation programmes. They must have access to clear and contextually appropriate advisory, governance and assurance assistance. They must also know which agencies provide which categories of information and at which point these agencies must or should be involved. Primary among those agencies are ASD and the DTA, both of which have key digital accountabilities. Both agencies could benefit from publishing a service catalogue to formalise their mandatory roles and advisory capabilities.

The ABS's interactions with ASD were not, in their eyes, straightforward. ASD provided varying levels of input to the ABS's solution, but the ABS interpreted the outcome of their meetings as endorsement of the eCensus approach. This view led to a level of confidence in the solution that was not warranted. The capacity of ASD to be the central point of cyber security governance and assurance in government has eroded, and agencies have never been more independent. This situation must be addressed. Consideration must be given to how to strengthen central governance and assurance, and this ownership may no longer logically sit with ASD, given their broader portfolio of responsibilities.

There is a whole-of-government approach to how digital services should be built. This is the Digital Service Standard (DSS), operated by the DTA. The ABS

was aware of the standard but chose not to opt into its provisions, as was their prerogative at that time (the DSS is now mandatory). The DSS provides a framework for conversations across key digital topics from security, accessibility and other technology standards to user-centric service design. The DSS should be matured and refined in order to specifically promote it as a pivotal assessment, governance and coaching tool.

The ABS's interactions with ASD and the Digital Transformation Office (DTO) illustrate how smaller agencies, and those whose IT procurement requirements are infrequent, can find the compliance and regulatory landscape confusing to navigate, and how they may contract with insufficient safeguards. There is no single, comprehensive source of truth to which agencies can turn to understand whole-of-government standards to which they or their vendors must or should comply, including procurement rules, technology requirements, and cyber- and data-security. For this reason, a central point of advice and governance should be established to assist agencies with the early stages of their digital initiatives. This may be a function of the central programme office detailed earlier. The 'RFP Ghostwriting Service' of the DTO's US counterpart, 18f, provides an example of how this can be successfully achieved.

Recommendation:

Consider how to strengthen central governance and assurance, and this ownership may no longer logically sit with ASD, given their broader portfolio of responsibilities.

Overhaul financial, procurement and contracting frameworks to support new ways of working with technology

At a macro level, current business case, funding, procurement and contracting frameworks all inhibit leaner, agile processes. Business cases must be modernised to accommodate digital programmes characterised by smaller, cheaper, incremental outcomes that are faster to deliver. Funding should move to a stage-gated model in which capital is released in tranches as project milestones are achieved: this model will allow for early identification and remediation of non-performing initiatives. Contracting frameworks that support agile programmes do not exist (and are equally scarce in the private sector) and the development of plain English agile contract templates must be a priority.

In relation to procurement practices, agency procurement processes that unnecessarily complicate the Commonwealth Procurement Rules (CPR) environment should be overhauled. The tension between panels and open tenders needs to be resolved, panel overlaps contained, and whole-of-government approaches to common ICT requirements formalised. The current procurement environment substitutes process compliance for a robust control environment. There is a belief that completing prescribed process steps will lead to a satisfactory outcome. As demonstrated by the ABS's decision to outsource to IBM - which passed a value for money assessment, a risk review and a probity review - this is not the case. In this instance, the very use of these process steps served to reduce the transparency of the procurement.

There is an unscoped but probably significant opportunity to improve operational ICT procurement processes. Procure-to-pay (P2) processes, even in

big agencies, can be underdeveloped compared to private sector counterparts, and paper-based. This will remain at least partly the case until e-signatures are approved for use in government contracting. Paperless e-invoicing processes also hold great potential for efficiency. A review of existing P2P environments is recommended, and many proven cloud-based offerings are capable of rapidly improving this space.

These changes will create greater transparency, efficiency and contractual protection for buyers. They will also lead to more inclusive procurement practices that will open procurement opportunities to a spectrum of non-traditional sellers who can apply leading-edge thinking to the government's ICT challenges. This will help break the cycle of dependence on large multinational organisations and encourage innovative domestic SMEs and start-ups into productive relationships with government. The recently announced Cyber Growth Centres and the Digital Marketplace both have roles to play in connecting government with sellers that have historically found it difficult to compete for public sector work.

Lastly, ICT procurement skillsets should be reviewed. The role played by the ABS's procurement team in the IBM outsource was that of a facilitator and did not display any understanding of key risks associated with a single tender action or more generally those associated with outsourcing. The success of all other changes in the ICT procurement sphere is ultimately dependent on the expertise of the procurement professionals tasked with their implementation.

Align policy and delivery more closely and allow citizens a choice of channels

Policy formulation and service delivery must be aligned more closely to each other. Closer alignment will entail changes to the way policy is enacted and handed down to delivery teams and will reverse changes introduced in the 1990s. The separation between policy and delivery makes it difficult to create the feedback loops that measure whether a policy is practically implementable, and whether service delivery meets the policy intent.

Stronger alignment of policy and delivery will make it easier to measure and to track the effectiveness and benefits of government services across all channels. This data should be freely available to citizens so that they can make informed choices about how they access services. Digital services should overlap other channels and not replace them, because unforced adoption is the true test of whether a digital service genuinely meets a need. An evidence-based, data-driven approach to digital services and digital service evolution should be adopted across government.

Accept that digital service delivery is iterative and will improve with citizen feedback and agency experience

It will be challenging but necessary for both government and citizens to accept the iterative nature of digital service delivery and to move away from "perfect" to "useful and available now". The public discourse must mature to the point where citizens are comfortable that services are initially released as "Minimum Viable Products" which offer useful functionality but are not polished and

require further development. Government, for its part, needs to become comfortable with the reality that some digital offerings will not thrive and that cheap fast-fail experiments that establish useful data points are features of new project delivery methodologies.

Government must acknowledge and resolve the contradictory needs of citizens regarding privacy, perhaps by looking to 21st century models of business success. These exemplars involve citizens sharing large amounts of personal data in return for benefits that are large enough for privacy to become a secondary concern. Government must focus effort on understanding these models of unforced adoption and should explore how behavioural economics can influence citizen uptake of digital services.

Privacy and security concerns, oppositional politics and negative media attitudes are likely to make a transition to more open government difficult and uncomfortable. They are also likely to limit government's ability to publicly share datasets. Recommendations on the public engagement that is required to advance the discourse are beyond the scope of this report.

Embracing a secure digital future - opportunities for Government

The ABS incident has undoubtedly cast a shadow over the prospects for e-government that is at odds with citizen expectations for more convenient and faster delivery of large-scale public services. An illustration of the current dichotomy is the community discontent with the length of time taken to finalise the paper-based federal election results.

A successful transition to a digital future will mean simpler, better services for citizens that are much more cost efficient. From a cloud perspective, eCensus represented a minor traffic challenge, equivalent to around 6 seconds of Facebook or 9 minutes of Twitter.

Digital service delivery models will de-risk initiatives by ensuring that the delivered outcome is relevant to the need and by accommodating the course corrections that user feedback will inevitably suggest. Open source protocols will permit domestic and transnational collaborations. Greater government transparency and citizen engagement will ensue.

Ultimately, this will permit initiatives such as the 2021 Census to be delivered in radically different ways.

Annex A: 2016 Census Taskforce Agencies

- Australian Bureau of Statistics
- Australian Government Solicitor
- Australian Signals Directorate
- Department of Finance
- Department of the Prime Minister and Cabinet
- Digital Transformation Office
- Office of the Australian Information Commissioner
- The Treasury