Submission to the Federal

Senate Standing Committees on Finance and Public Administration

DIGITAL DELIVERY OF GOVERNMENT SERVICES

Table of Contents

Contact details:
Ian Brightwell

File: Submission - Digital delivery of government services - Final.docx

Recommendations

The author commends the following recommendations for the Committee's consideration.

Recommendation 1

The committee recommend to government that a consensus be developed which defines "acceptable failure" for an agency ICT program.

Recommendation 2

The committee recommend to government that they should undertake Gateway Reviews and Implementation Readiness Assessments for all major or high-risk public facing ICT programs.

Recommendation 3

The committee recommend to government that they direct DTA to extend their Performance Dashboard *to include the program status items similar to the* Queensland Government ICT Project Dashboard*.*

Recommendation 4

The committee recommend to government that ICT governance in agencies only allows the delivery of public facing transactional systems where the system (including the infrastructure) is independently determined to be able to meet community expectations of security, reliability and performance.

Recommendation 5

The committee recommend to government that agencies separate the role of CIO and CISO and ensure that each role has a separate reporting line to the agency CEO.

Recommendation 6

The committee recommend to government that they provide incentives for agencies to broaden use of their business information systems to allow other agencies (including state agencies) to take them up as-a-service.

Executive Summary

The government's policy to move to a digital economy is a necessary for the prosperity of our nation. However, this strategy is not easy to implement and will reveal many weaknesses in the way government currently manages ICT programs and indeed programs in general.

I contend that the problems we see with the delivery and management of ICT systems within government is not so much about the Australian Public Sectors (APS) inability to deliver ICT programs but rather a reflection of the APS's ability to delivery programs in general. The reason ICT program failure appears to be becoming more prevalent is because the APS is now undertaking the implementation of more public facing online systems which have higher visible and irrefutable failures. This means the public and media are more easily able to identify agency program failures. Also, ICT programs are typically more fragile and will fail if only one piece of the system does not work were traditional programs tend to be more robust.

Online service delivery to the public is a relatively new environment for the public sector, which typically has operated in an environment where most program weaknesses or failures can be obscured behind the difficulties of measuring performance of paper based systems. Operational statistics for these systems are rarely provided and if provided by FoI the data is heavily redacted on privacy or contractual grounds.

The following are areas covered by this submission:

- Increased ICT program assurance
- Greater visibility of ICT program status and operational status
- Guidelines for "acceptable failure"
- Improved agency governance of enterprise ICT
- Segregation of duties wrt ICT management and the measurement and reporting of non-functional requirement such as security
- Improved platform utilisation including by states

1 Author Background

The author of this submission is a consultant, adjunct faculty member at UNSW[1] and experienced CIO. He helps clients better manage and utilise their technology investments. He specialises in program and portfolio management and technology governance with a particular focus on information security.

In addition to postgraduate qualifications in information systems and management he is Certified by ISACA[2] in the Governance of Enterprise IT (CGEIT)[3] and a trained Gateway Reviewer for NSW ICT programs.

He provides advice to organisations on how to improve their technology and program governance. Is a gateway reviewer for government providing program assurance advice. Also provides executive advice on how organisations can effectively and efficiently improve their security posture.

He was CIO and Director of IT at the New South Wales (NSW) Electoral Commission in Australia. Responsible for the provision of all IT infrastructure and information security for the Commission and led NSW award winning electronic voting initiative (iVote) at the 2011 and 2015 elections[4].

More details can be found on linkedin[5].

[1] This adjunct title was conferred for contributions to the academic activities of the School of Computer Science and Engineering, Faculty of Engineering at the University of NSW.

[2] Information Systems Audit and Control Association, ISACA
http://www.isaca.org/about-isaca/Pages/default.aspx

[3] Governance of Enterprise IT (CGEIT)
https://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Pages/default.aspx

[4] Australian Government ICT Awards Program 2016
http://www.finance.gov.au/archive/australian-government-ict-awards-program/australian-government-ict-awards-program-2016/

[5] https://www.linkedin.com/in/ian-brightwell-a038573/

2 Program Assurance and Transparency

Dr Parkinson the Secretary of the Department of the Prime Minister and Cabinet gave a speech[6] last year at IPAA[7] Annual Address to the Public Service. In that address he acknowledged the need to improve rapidly the service delivery of by the Australian Public Service (APS):

> *Disruptive forces—like the fundamental shift in public expectations of government, consumer-directed demand for government services and the ever-changing capacity of technology to support and improve service delivery—are certainly not unique to the public sector. Indeed, they impact on our work just as much as they impact on the private sector.*

He also suggested the APS did not understand disruption:

> *But despite this, it seems to be that in the APS we think that disruption is something happening to other people. And, conversely, we seem to regard innovation as a buzzword or something that's 'nice to have'.*

Additionally, he expressed concern the APS would not respond appropriately to the challenge:

> *But one thing that has surprised me is the complacency, yes, complacency, which many in the public service have regarding the disruptive forces operating around us.*
>
> *I want to be clear—this is a false reality. And a dangerous one at that. And it feeds into my concern that the APS is at risk of the* ***fatal combination of arrogance and ignorance****.*

I agree with the above observations and concerns of Dr Parkinson. It has been my observation that the APS has had the tendency to hide from public scrutiny by using confidentially, privacy and secrecy whenever programs have failed to meet their stated objectives. They have been successful in avoiding criticism for program failures for traditional highly manual public service programs because performance for these programs is hard for external parties to measure. This difficultly to measure is not the case for many online ICT programs. In these programs failure is easy to identify and the public can readily see if the delivered system works or not.

The APS is not comfortable to being in a position where they have the same information in their hands as the public. They do not deal well with the public and media scrutiny when they are being criticised with facts they cannot refute. One of the reasons they do not do well in these situations is because they are between a "rock and a hard place" when coming before committees like this Senate committee. The nature of the committee process is political and seeks to extract information from the APS which can be used to damage political opponents. If parliament at large want the APS to be innovative and take risks then parliament will need to set some ground rules around what is acceptable risk and what does acceptable failure look like. If this is not done then the APS will simply

---

[6] IPAA Annual Address to the Public Service, Martin Parkinson, Secretary of the Department of the Prime Minister and Cabinet, 6/12/2016
https://www.pmc.gov.au/news-centre/pmc/annual-address-public-service

[7] Institute of Public Administration Australia (IPAA)
http://www.ipaa.org.au/

"play cat and mouse" whenever anyone accuses them of any type of failure. They will obscure key information which could provide valuable learning for other agencies and parliament. In short, they currently have not incentive to deal with anyone outside their organisation openly.

Recommendation 1

The committee recommend to government that a consensus be developed which defines "acceptable failure" for an agency ICT program.

The only way to improve decision making about programs is for more information about program health to be shared openly. The best way to get objective information which could be shared is for agency programs to undergo independent reviews. Currently agencies do undergo a limited number of structured reviews in the form or Gateway Reviews and Implementation Readiness Assessment.

The outcome of these Gateway reviews are currently not shared widely within or outside government. I would suggest findings from information should be shared more widely to improve the public and parliament's understanding of the causes and extent of program failures. A way of achieving this is of the review data to be published on the DTA's new program status dashboard. A recently published report from the ICT Procurement Reform Taskforce[8] said in Recommendation 4 the government should support the development of "a dashboard of ICT spending which will be accessible to government and government agencies".

I would contend this recommendation is too narrow and the dashboard should not be limited access by only government agencies is should be public and include program status and progress in a similar manner to the Queensland government's dashboard[9]. Queensland learnt the very hard way that the best course of action is to be open and transparent. Will the Commonwealth have to learn the same lesson over again? I argued for greater transparency in an article I wrote earlier this year[10].

It is also interesting to note that a recent ANAO report also recommended the use of improved traffic light reporting showing publicly the progress of NISA projects[11].

Recommendation 2

The committee recommend to government that they should undertake Gateway Reviews and Implementation Readiness Assessments for all major or high-risk public facing ICT programs.

[8] Government response to report of the ICT Procurement Reform Taskforce
http://ict-procurement.digital.gov.au/response.html

[9] Qld ICT Dashboard
https://www.qld.gov.au/ictdashboard

[10] Governments must be more transparent about ICT project statuses, CIO Magazine, Ian Brightwell (CIO) 24 February, 2017
https://www.cio.com.au/article/614785/governments-must-more-transparent-about-ict-project-statuses/

[11] Design and Monitoring of the National Innovation and Science Agenda, September 27, 2017, ANAO
https://www.anao.gov.au/work/performance-audit/design-and-monitoring-national-innovation-and-science-agenda

Recommendation 3

The committee recommend to government that they direct DTA to extend their Performance Dashboard to include the program status items similar to the Queensland Government ICT Project Dashboard.

In summary, the reason ICT program failure appears more prevalent is because public facing online system failures are more visible hence are much easier for the public and media to identify and by their nature irrefutable. Also, ICT programs are typically more fragile and will fail if only one piece of the system does not work were traditional programs tend to be more robust. This in part is why many agencies are reluctant to build these systems as they know there is a reasonable probability they will fail and the agency and CEO will be exposed to public ridicule.

The reasons for failure are many and varied. They range from lack of ICT planning and delivery skills to poor backend infrastructure and systems upon which to build online systems. I will discuss some of these issues in subsequent sections of this submission.

3 Governance and Digital Transformation

There is gap between ICT management's and by extension general management's perception of their organisations capability to support digital services compared to that of staff in ICT operations roles. A recent survey[12] by PageDuty in Australia found:

> *a perception gap among the leaders of IT, developer and DevOps teams and the people responsible for addressing digital service performance issues. Within the group of respondents who cited confidence in their organisation's ability to support digital services, 31.8 percent were in management roles, representing the largest group. Only a combined 5.2 percent of development team leads (2.6 percent) and those in an infrastructure role indicated their organisation is prepared.*

The response to the survey clearly shows that the people at the ICT "coal face" are not as comfortable as management in their organisation's ability to support digital services. Interestingly the same survey identified that:

> *the most critical challenges their IT organisation is facing as a result of the rise in digital services, IT personnel cited*
>
> - *increased difficulty in capacity planning (e.g., increase in volume of data),*
> - *increased complexity resulting in more cognitive load, an*
> - *increase in the number of tools and as the top operations challenges.*
>
> *IT organisations are also challenged with reduced budget, lack of full stack visibility, lack of contextual data when troubleshooting, siloed IT functions limiting collaboration and alert fatigue.*

[12] Australian State of Digital Operations Report, https://www.pagerduty.com/resources/reports/digital-operations-aus/

Finally, IT organisations identified that the ICT group:

> *most responsible for ensuring seamless delivery and performance of their digital offerings—DevOps, development or IT Operations—more than half of respondents (55.7 percent) selected* ***IT Operations****.*

The above gap illustrated above shows that many organisations are facing the same problem, which is an inability to convey technical decisions to the right level of decision maker. I have noted during my career that a large number of key decisions effecting system reliability and security are often made at a very low technical level without consultation with more senior managers and without proper consideration of consequence. This happens for a range of reasons including expedience and the inability and unwillingness of technical people to convey these issues to others in a meaningful and timely manner.

It is important to note that many of the people who are making these decisions at a technical level are often contractors who are on short term assignment and have little knowledge of the organisations decision making processes. These people are often supervised by agency staff who have little appreciation of the technology they have responsibility for managing. This is a fatal combination because the supervisor is unable to effectively communicate with the contractor who is incentivised the complete the task as quickly as possible.

The only real solution is to improve technology governance and introduce methodologies which ensure that decisions are made in accordance to agency policies. This is not easy and requires a lot of education and cultural change.

In addition to the need for improved governance systems agencies need to undertake more independent reviews of internal operations. Management needs to be certain that the governance systems are working and that key decisions are flowing up the line to be dealt with by the right manager. This is particularly critical for system which are public facing.

> **Recommendation 4**
>
> *The committee recommend to government that ICT governance in agencies only allows the delivery of public facing transactional systems where the system (including the infrastructure) is independently determined to be able to meet community expectations of security, reliability and performance.*

4 Segregated Security Reporting Lines

Independ advice on cyber security vs ICT operations from inside of agencies is critical to improve decision making. Agencies are typically structured on functional lines, with ICT and cyber security often placed under one functional arm within agencies. This approach has the disadvantage of limiting the potential for difficult security decisions being elevated outside of the ICT area of the organisation.

The ABS failure was a clear case where the decision to accept “Island Australia” as an acceptable solution to DDOS attacks was clearly flawed. I recently assessed the ABS security roles in an article

for CIO magazine and questioned whether ABS had learnt anything from its e-Census debacle[13]. ABS had a combined CIO/CISO role and this role made key decisions about security and operations without necessary exposing the thought processes for the scrutiny of other managers or executives. The Australian Statistician acknowledged that a lack of reliable information being provided to senior management was one of the causes of the debacle. However, this did not stop them advertising after the Census for a person to again fill the combined CIO/CISO role.

It is interesting to note that the AEC has also advertised a combined CIO/CISO role recently and therefore risks the same problems experienced by the ABS.

Recommendation 5

The committee recommend to government that agencies separate the role of CIO and CISO and ensure that each role has a separate reporting line to the agency CEO.

5 Improved Platform utilisation

A recent report[14] by the DTA on ICT procurement identified that there is a need to better exploit the use of ICT platforms across government agencies. This has the obvious benefit of reducing replication of effort and infrastructure by using functionality which already exists in other agencies. This is a sensible recommendation but not necessarily easy to implement.

There has been some success in this area with development of platforms like GovCMS[15], which has proved to be very popular with many agencies including state agencies. GovCMS provides agencies the ability to build a website using a preapproved tool and tested hosting. The are other areas of ICT usage within government which could benefit from this type of initiative are email and other communication and collaboration platforms.

I believe there is a need however for the Commonwealth to examine the viability of providing or facilitating the provision of ICT business platforms which can be used at all levels of government. This approach is one which would the Australian economy the greatest benefit. The greatest expenditure by the Commonwealth on ICT is in the provision of business systems not the licencing of off the shelf desktop products. There are a number of agencies which have common business system needs at the state and federal level. An example is in the electoral area where the AEC and state Commissions perform very similar tasks.

The AEC is currently seeking significant funding to upgrade all its systems. This will be a major project and will no doubt be done using a technology base which could be leveraged by state Commissions. The savings are obvious should this sharing of resources be successful. However, the likelihood of it succeeding, if the AEC is the controlling agency is very low. Governance of this type of

[13] Opinion: Has the ABS learnt anything from its e-Census DDoS debacle?
https://www.cio.com.au/article/614212/opinion-has-abs-learnt-anything-from-its-e-census-ddos-debacle/

[14] Report of the ICT Procurement Taskforce, Digital Transformation Agency. Report of the ICT Procurement Taskforce. Canberra: Commonwealth of Australia. May 2017
http://ict-procurement.digital.gov.au/assets/documents/ICT-procurement-taskforce-report_WCAG.pdf

[15] GovCMS https://www.govcms.gov.au/

project is the key to its success and as such a separate entity with shared governance would need to be established. Such and entity could manage the processing of rolls, election funding, election management and even online voting for those jurisdictions which allow it.

An example of a suitable entity is demonstrated by the PSMA[16]. PSMA Australia Limited is an unlisted public company owned by Australia's federal, state and territory governments. Our goal is to facilitate broad and sustainable access to high-quality location data. This type of ownership and governance could provide a shared services model for many areas of government in Australia.

Recommendation 6

The committee recommend to government that they provide incentives for agencies to broaden use of their business information systems to allow other agencies (including state agencies) to take them up as-a-service.

[16] PSMA about page
https://www.psma.com.au/about