Submission to the Department of Prime Minister & Cabinet on the ICT Procurement Task Force's consultation paper

Safecoms Cyber Security Pty Ltd

in association with

Holden Dynamics Pty Ltd

and

South Australian Open Source Consulting Engineers

Saosce Pty Ltd

Lodged 31 January 2017

Authors
Jack Burton & Carl Holden.

Contacts
For further information in relation to this document, contact Jack Burton, Company Secretary, Safecoms Cyber Security Pty Ltd by email at <jack@safecoms.com.au> or by telephone on (08) 8121 3075.

Please cite this work as:
Burton, J. & Holden, C., *Submission to the Department of Prime Minister & Cabinet on the ICT Procurement Task Force's consultation paper*, Safecoms Cyber Security, Adelaide, January 2017.

About the companies

Safecoms Cyber Security Pty Ltd

Safecoms Cyber Security is a new & exciting Australian start-up in the information security sector, founded in 2016 by industry veterans Carl Holden & Jack Burton. Safecoms has three divisions:

The consulting division is the centrepiece of the company, leveraging the founders' combined expertise and more than half a century of industry experience to deliver the full spectrum of information security advisory services including strategic infosec consulting, systems audits, code audits, penetration testing, critical incident response and forensic analysis.

The secure cloud services division, led by Mr Burton, aims to bring the peace of mind traditionally associated with rock-solid enterprise computing and secure-by-design development methodologies to a range of specific cloud-based services. The first such initiative is scheduled to be launched during 2017.

The automotive division, led by Mr Holden, seeks new & innovative ways to address the severe cyber-security issues that plague today's advanced automobiles. Focussed on research & development at present, the first such initiative is expected to go to market in 2018.

For further information, see the Safecoms website at `https://safecoms.com.au`.

Holden Dynamics Pty Ltd

Holden Dynamics was founded by Mr Holden in 1987 to work with innovative technologies to enable his committment to "making a difference", through the use of innovative technologies.

Holden Dynamics has been involved in the introduction to Australia of personal communications (CB radio) and personal aviation (ultralight aviation) and foeresaw the need for infosec as far back as 2000, when it spun off another start-up company for that purpose.

They help many businesses, mainly SMEs, including with coaching. Today, Holden Dynamics operates in diverse fields and holds Defence Supplier Code Z03G2.

For further information, see the Holden Dynamics website at `https://holdendynamics.com`.

Saosce Pty Ltd

Saosce is an acronym for South Australian Open Source Consulting Engineers. Based in Adelaide and founded in 2002, Saosce is a full service computing consultancy & services firm, blending the complementary disciplines of computing and management consulting to provide comprehensive advice and end-to-end solutions tailored to each client's specific business needs.

Saosce focus on Unix and open source software, but within that field cover the full gamut of services, including strategic consulting, business analysis & modelling, software development, technical documentation, information security, information & technology governance and business continuity.

Their clients have ranged in size from ASX100 companies to microbusinesses and have been drawn from a diverse range of industries, as well as organisations in the public sector and not-for-profit sector.

For further information, see the Saosce website at `https://saosce.com.au`.

About the authors

Jack Burton BSc MACS CP

Jack Burton has been involved in commercial computing since 1989, beginning in Fortran programming and later database design, leading—after interludes in sales management & management consulting—to ICT management and eventually computing consultancy. Mr Burton is currently Director of Saosce Pty Ltd, a firm he founded in 2002, and Director & Company Secretary of Safecoms Cyber Security Pty Ltd, a firm he & Mr Holden jointly founded in 2016.

In addition to his commercial activities, Mr Burton has undertaken a large amount of pro bono service over the years, for a variety of computing-related industy bodies & professional societies, including Open Source Industry Australia Ltd (OSIA: 2007 & 2010–2016), OpenSA Inc. (2009–2013) and the Australian Computer Society Inc. (ACS: 2007–2013).

He is well known throughout the Australian computing profession and in particular within the Australian open source software industry.

Mr Burton holds a Bachelor of Science from Monash University and is a Member of the Australian Computer Society, Certified Professional. He also maintains professional membership in the Association for Computing Machinery (ACM, USA), the American Society for Quality (ASQ, Software Division), the Information Technology Professionals Association (ITPA, formerly SAGE-AU) and the Telecommunications Association (TelSoc).

Carl Holden MSAE AACS

Carl Holden's first foray into computing was in the 1970s, maintaining CP/M based equipment running Microasis software. Mr Holden is currently Managing Director of Holden Dynamics Pty Ltd, a firm he founded in 1987, and Chairman of Safecoms Cyber Security Pty Ltd, a firm he & Mr Burton jointly founded in 2016.

In addition to his commercial activities, Mr Holden has undertaken a wide range of pro bono service over the years, for a variety of industry bodies, including Open Source Industry Australia Ltd (OSIA: 2010–2013) and The Oaks Chamber of Commerce (2000–2016, which he founded).

He is very passionate about technology and "making a difference".

Mr Holden is a Member of the Society of Automotive Engineers and an Associate of the Australian Computer Society. He also maintains professional membership in the Association for Computing Machinery (ACM, USA), the Armed Forces Communication & Electronics Association (AFCEA, USA), the Australian Information Security Association (AISA) and the Information Security, Audit & Control Association (ISACA).

Relationship to other submissions

Holden Dynamics Pty Ltd and Saosce Pty Ltd are both members of Open Source Industry Australia Ltd (OSIA)[1], the industry body representing open source software companies in Australia. Both authors of this submission were former directors of OSIA.

We are aware that, as at November 2016, OSIA was intending to lodge its own submission to the task force. We are not aware of whether or not OSIA has lodged such a submission and if it has we are not privy to its contents, nor has the current OSIA board been privy to the contents of this submission prior to lodgement.

For clarity, please note that the authors of this submission **do not** speak for OSIA.

Nevertheless, during our respective tenures at OSIA—and in Mr Burton's case also formerly at OpenSA—we have each had a great many conversations with a wide range of those organisations' member companies on the subject of government procurement. It is natural therefore that, where relevant, we draw on those experiences in addition to those of our own companies.

[1] http://osia.com.au

Contents

1 Executive summary

The authors welcome the opportunity to comment on the discussion paper and we thank the task force for that opportunity.

We support the task force's objectives of increasing innovation in government ICT generally and in government ICT procurement in particular, in order to deliver better government services at lower costs and to make it easier & cheaper for industry to do business with the Commonwealth.

Furthermore we agree with the task force that increasing SME & start-up involvement in the government procurement marketplace will help drive innovation in government ICT. Ideally, innovation in industry should drive innovation in government and SMEs & start-ups are generally where most innovation in industry is found.

In our view, there are ten key areas on which the task force should focus:

- Increasing dramatically the use of Free[2] & Open Source[3] Software (FOSS) in government generally, but most importantly in those areas of ICT in which the Commonwealth has to date not taken advantage of the many benefits that FOSS offers;
- Releasing publicly all non-classified software developed by or for the Commonwealth under FOSS licences. This and the previous item could both best be addressed by improving or replacing the rather timid existing Australian Government Open Source Software Policy, to bring it into line with best practices overseas, or better still to put Australia in a world-leading position;
- Applying a more open, innovative mindset to ICT projects in government generally and adopting some novel & innovative approaches to ICT procurement processes & practices specifically;
- Reducing barriers to entry for SMEs & start-ups, specifically by easing financial viability criteria for those suppliers proposing software solely under FOSS licences;
- Removing the artificial constraints that currently prevent the Commonwealth from implementing a policy of local preference in ICT procurement, to bring procurement policy in line with the Government's new "Australia first" trade policy;
- Engaging more proactively with relevant, innovative SMEs;
- Adopting a "security first" approach to procuring cloud services;
- Amending the approach to assessing migration costs to ensure that proposals are evaluated on their own merit (rather than in part on the merit of their predecessors);
- Decentralising responsibility and authority for decision-making, whilst centralising shared knowledge and putting in place processes to encourage agencies to share information about novel & innovative ICT solutions & approaches to ICT procurement; and
- Increasing transparency in procurement and abolishing all remaining anti-competitive procurement arrangements.

Should the task force desire any further information or clarification of any of the matters raised in this submission, please feel free to contact us directly. We would welcome any further involvement in the work of the task force, which we see as highly important to the future of ICT in government.

1.1 Structure of this submission

The following section lists all of our recommendations. For the remainder of the document, we address the issues in order in which they arose in the discussion paper, following the structure of that paper.

[2] "Free Software" has nothing to do with price. In this context, "Free" refers to *freedom*, specifically, four essential freedoms that a software licence must bestow on the licensee, as described in the Free Software Definition. See Stallman, R., *What is Free Software?*, Free Software Foundation. Available at http://www.gnu.org/philosophy/free-sw.en.html

[3] Perens, B., *Open Source Definition*, Open Source Initiative, 1998. Available at http://opensource.org/osd

1.2 Recommendations

The recommendations below are listed in the order in which they appear in the main text of this submission. The numbering of recommendations is for ease of reference only and is not intended to imply any order of priority.

The authors recommend that the Commonwealth Government:

1. End Source IT's effective mandate for COTS software.
2. Revise the APS ICT Strategy, introducing specific actions to invest in FOSS[4] to transform services & achieve savings.
3. Approach the market with each set of *business needs*, seeking free-form proposals for novel & innovative approaches to meeting those needs, *prior* to any regular procurement exercise commencing.
4. Decentralise authority for decision-making and responsibility for approaching the market to seek novel & innovative solutions, but create a central repository of shared knowledge about all computing solutions across government and institute processes & practices to foster information sharing & collaboration between computing personnel across all agencies.
5. Signal more clearly in the marketplace the Commonwealth's desire to increase greatly the proportion by value of its ICT contracts awarded to SMEs.
6. Lower the supplier financial viability criteria substantially for any contract in which the supplier guarantees that all software supplied will be licenced to the Commonwealth under terms which comply with the Free Software Definition[5], and/or the Open Source Definition[6].
7. Focus on seeking novel & innovative solutions in those areas in which the least innovation has occurred in recent times and which also account for the lion's share of Commonwealth ICT spend.
8. Establish a policy of never ratifying or acceding to any treaty which prohibits local preference in public procurement and renegotiate all such existing treaties without the offending provisions.
9. Overhaul the Australian Government Open Source Software policy, at the very least to bring it into line with the rest of the world, ideally to place Australia in a world-leading position. Ideally the revised policy should include:
   (a) a firm preference for open source software, coupled with a requirement for detailed justification & external review before an agency may procure software under any licence that fails to grant the rights of modification & redistribution; and
   (b) a requirement that all non-classified software developed by or for the Commonwealth be released publicly under licenses compliant with the Free Software Definition and/or the Open Source Definition.
10. Enforce consideration of *exit* migration costs in the evaluation of all ICT proposals & tenders.
11. Prohibit the procurement of any software which fails to adhere to the relevant unencumbered open standards for all data storage & communication.
12. Make all agency-specific procurement rules publicly available.
13. Use genuinely competitive processes for procuring all desktop software (and all other classes of software currently covered by the MVSA).

[4] Free & open source software

[5] Stallman, R., *op. cit.*

[6] Perens, B., *op. cit.*

2 Overview

2.1 Collaboration, acquisition models & FOSS

This paper's authors agree with the discussion paper's assertion (at p. 2) that "[c]urrently, collaboration between government and industry to develop ICT solutions is limited". There is definitely more scope for collaboration between government and industry to *develop* solutions (as opposed to merely accepting existing ones). This is one area in which the Commonwealth could learn a lot from the open source software development model.

In a legacy, closed source world, end users (including Commonwealth agencies) need to make traditional "buy versus build" decisions: either they purchase licences for off-the-shelf (OTS) software, which entails a conscious decision to accept any and all limitations baked into that software; or they develop software to meet their specific needs exactly (possibly in-house, or possibly by engaging an external company to do so), which entails a conscious decision to foot the bill for ongoing maintenance of that software, for the entirety of its useful life.

Many Commonwealth agencies appear to be stuck in that obsolete paradigm. The trouble is that *both* of those options lead to lock-in, by restricting severely the number of organisations capable of providing ongoing support & maintenance programming. In the case of OTS closed-source software, *only* the original software vendor itself is capable of providing those services comprehensively.

The risk of "built" bespoke closed source software becoming orphaned is substantial. For example, a particular State library engaged a local company to develop a bespoke system in Java. Six months later the local company went bankrupt leaving the library with no technical support and no right to modify the source code as the system had been procured under a closed source software licence.

The greatest issue with "bought" OTS closed source software is the absence of the right to modify the code to meet the exact needs of the organisation as they evolve over time. In addition to licensing issues, OTS closed source software tends to suffer from limitations on compatibility: often it is only compatible with other software from the same vendor—one common tactic that some nefarious vendors use to achieve vendor lock-in.

A key risk today (even more so than in the past) is the rapid turnover in OTS closed source software products and obsolescence. As OTS closed source software products attempt to keep up with the disruption caused by free & open source software (FOSS), agencies find themselves lumbered with more and more (often incompatible) products with little to no adaptability. This adds to an ever increasing software maintenance cost for the Commonwealth and the taxpayer.

On the other hand, the approach taken in the FOSS world is a far more efficient & cost-effective one—and one which by its very nature is conducive to collaboration with industry: to start by acquiring software which meets *most* of the agency's needs under a licence which permits modification & redistribution (as all FOSS licences do[7]), ideally at zero cost, then improving that software so that it meets *all* of the agency's need exactly and contributing those improvements back to the relevant maintainer(s).

The cost reduction benefits of such an approach are clear: usually no licence fees are payable; the cost of incremental development (whether undertaken in-house or outsourced to a suitably competent company) is often less than the cost of licensing similar closed source software; and assuming that the improvements contributed back are accepted upstream, the cost of ongoing maintenance programming is effectively borne by the software's maintainers and/or community.

As an added bonus, being permitted (or better still encouraged) to contribute improvements back to publicly maintained FOSS projects tends to have a positive effect on the morale and motivation of in-house developers, as it gives them the opportunity to see their work have a positive effect globally (in addition to its positive effect on the agency's initiatives & their beneficiaries).

But the associated flexibility is where the greatest benefits lie: the ability to have the software meet the agency's *exact* needs (not just "close enough" as is often the best that can be achieved with closed source software) without incurring the substantial costs of development from scratch; and the ability to innovate and to have the software keep pace with that innovation, in near-real-time.

As one industry commentator put it, "unless managed carefully, a naive approach to implementing COTS software can fail to deliver on its core promises of lower costs and reduced complexity. It can also stifle innovation"[8].

[7] Stallman, *op. cit.*; Perens, *op. cit.*

[8] Corrigan, B., *How COTS became Australia's default software setting*, ITNews, NextMedia, 25 Mar 2014. Available at: http://www.

The Gershon Review[9] recommended a preference for "commercial off-the-shelf" (COTS—roughly equivalent to OTS closed source) software, but that recommendation is no longer tenable. Arguably it has made no impact on costs or complexity while stifling innovation.

In recent times the Commonwealth's approach has been what effectively amounts to a mandate for COTS software through the provision of the Source IT[10] model contract for COTS[11] without providing the same level playing field for FOSS that is prevalent in the USA, the UK & the EU.

To reverse this concerning trend, the Commonwealth would be well advised to institute a policy of acquiring software *only* under licences which grant the rights to modify and to redistribute. Those criteria (and others) are met by all licences compliant with the Free Software Definition and/or the Open Source Definition. Such a policy could be implemented as part of a long-overdue review of the Australian Government Open Source Software Policy—see Section 4.1.

Governments do occasionally still encounter requirements to develop software from scratch, especially when undertaking innovative initatives that may be world firsts. When such requirements arise, there is still considerable benefit to be derived from releasing the software under a FOSS licence.

Once the initiative launches successfully and becomes well known, chances are other governments (and in some cases corporations or even individuals) may see value in the software, start using it and start contributing back their own improvements (be they bug/security fixes or feature enhancements).

For the developing agency post-launch, this creates the potential to reduce ongoing spend on maintenance programming and the potential for the Commonwealth to build a reputation as an innovative, world-leading government (both in public policy development and in its approach to software procurement).

The Commonwealth would be well advised to institute a policy of requiring that all non-classified software developed by or for Commonwealth agencies be released publicly under licences compliant with the Free Software Definition and/or the Open Source Definition. Again, such a policy could be implemented as part of a long-overdue review of the Australian Government Open Source Software Policy—see Section 4.1.

Recommendation End Source IT's effective mandate for COTS software.

On reviewing the APS ICT Strategy[12], we were amazed to discover that it makes no reference whatsoever to FOSS, nor to open systems nor open data and it makes only one brief reference in passing to open standards[13]. In contrast, even such a relatively obscure agency the UK Veterinary Medicines Directorate does a better job of providing leadership in procurement by "using free or open source where applicable"[14]!

Recommendation Revise the APS ICT Strategy, introducing specific actions to invest in FOSS to transform services & achieve savings.

itnews.com.au/feature/how-cots-became-australias-default-software-setting-375927

[9] Gershon, P., *Review of the Australian Government's use of information and communication technology*, AGIMO (Department of Finance & Deregulation), 2008. Available at: https://www.finance.gov.au/sites/default/files/Review-of-the-Australian-Governments-Use-of-Information-and-Communication-Technology_1.pdf

[10] http://www.finance.gov.au/policy-guides-procurement/sourceit-model-contracts/sourceit-software1/

[11] Whilst the Source IT model contract for COTS does include provisions for open source software licensing, they appear to be more of an afterthought than anything else. Reading the accompanying materials (and even the main heading on the Source IT web site!) gives one the distinct impression that the model contract is intended mostly for COTS software, with FOSS-specific provisions presumably intended to apply only to ancillary software distributed together with the principal COTS software.

[12] AGIMO, *Australian Public Service Information and Communications Technology Strategy 2012 – 2015*, Department of Finance & Deregulation, 2012. Available at: http://www.finance.gov.au/files/2013/01/APS_ICT_Strategy.pdf

[13] *Ibid.*, p. 19.

[14] Veterinary Medicines Directorate, *VMD Information & Communications Technology (ICT) Strategy 2016/2017*, Department of Environment, Food & Rural Affairs (UK), 2016. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/544343/_463375_VMD_Strat_010_A_-_VMD_Information___Communications_Strategy.pdf

2.2 Unsolicited proposals

The discussion paper goes on to note that currently, “unsolicited proposals may not be given full consideration”.

When an *actual need* arises and is recognised within government as having arisen (as often happens), we agree with the sentiment implied by the discussion paper that there is often insufficient attention paid to seeking novel & innovative proposals from the market.

Ideally, innovation in industry should drive innovation in government. So there may well be considerable value in instituting a policy of going to market for novel & innovative approaches of addressing agencies’ specific *business needs* as and when they’re anticipated to arise (as opposed to requests for proposals or tenders couched in highly prescriptive terms, where the “solution”—although not who will deliver it—has effectively been mandated prior to the approach to market), i.e. competitive consulting arrangements for a set fee.

See also our comments in Section 5.2.

Recommendation Approach the market with each set of *business needs*, seeking free-form proposals for novel & innovative approaches to meeting those needs, *prior* to any regular procurement exercise commencing.

2.3 On the “risk of duplication”

The discussion paper also notes that “agency decisions focus on agency-specific solutions rather than whole-of-government solutions, increasing the risk of duplication”.

The debate about centralising versus decentralising the control and management of computing in large organisations (including governments) has been ongoing for some decades. There is no consensus view, either in industry or in government. Advocates for centralisation argue that it is paramount to achieve economies of scale in any form of procurement: this is where the “risk of duplication” comes in.

Advocates for decentralisation argue that it is paramount to maximise flexiblity, such that in every case the software in use is the best fit for the agency using it and that innovation comes more naturally under the decentralised model, as the existence of multiple alternative solutions fosters healthy competition between the staff responsible for those solutions in each agency or division, as agencies over time adopt each other’s solutions on merit (cf. by central decree), so long as agencies *routinely share* information with each other about the solutions that they’ve developed or procured.

This paper’s authors tend to fall into the latter camp, although we do acknowledge that the decentralised approach requires far more mature computing capabilities & culture across all participating agencies. In our view, the goal should be to centralise *shared knowledge* about government computing projects but to decentralise their acquisition, development, assessment, selection & adoption. Such an approach strikes a good balance between the need for information sharing and the need to foster innovation.

We had hoped that the Open Technology Foundation (OTF) would make that vision a reality, across all governments in Australia & New Zealand (indeed in 2009 one of this paper’s authors was tangentially involved in the early planning for its establishment and we both attended its launch with great enthusiasm in 2011). Unfortunately, it appears that for a number of years OTF struggled to deliver on its highly ambitious mission. A far more achievable target would be to establish that same model within a single government, ideally the Commonwealth. Naturally, such an initiative would require a champion committed to its success.

Recommendation Decentralise authority for decision-making and responsibility for approaching the market to seek novel & innovative solutions, but create a central repository of shared knowledge about all computing solutions across government and institute processes & practices to foster information sharing & collaboration between computing personnel across all agencies.

2.4 Acquisition models revisited

The discussion paper asserts: “Into the future, the Government’s ICT procurement decisions must consider whether the best quality service can be provided by: owning the solution, partnering for the solution, or providing the solution via high-quality interfaces." Respectfully, we must disagree. In our experience the best solutions tend to *combine all three* of those models. There is no need for explicit delineation between them.

In Section 2.1, we outlined the benefits of developing improvements to software developed elsewhere & contributing those improvements back upstream and the benefits of releasing in-house developed software publicly under FOSS licences.

"High-quality interfaces" are just as important in software that is procured or developed in-house as they are in software accessed "in the cloud". Interoperability is more important now than ever before and that trend will only continue into the foreseeable future. This is an area in which the exclusive use of unencumbered open standards is paramount. See also our comments in Section 4.2.

2.5 Response to specific questions

> *1. How can the Australian Government make better use of ICT procurement to increase innovation in government services? What are the incremental and more transformational changes that could be made?*

Whilst procurement is a key factor, we suggest that the goal should rather be to determine how Government can make better use of ICT (whether procured, developed in-house, or acquired in some other manner). As noted above, hybrid acquisition models are undoubtedly the way of the future. The Commonwealth should be exploring various broader approaches for collaboration with industry.

A good start would be approaching the market with each set of *business needs*, seeking free-form proposals for novel & innovative approaches to meeting those needs, prior to any regular procurement exercise commencing (i.e. competitive consulting engagements). See also our comments in Section 5.2.

A suitably championed initiative to foster sharing of information (but not necessarily of implementations) between the agencies would be of great help too. See also our comments in Section 2.3.

A policy of acquiring software exclusively under FOSS licences would also make an enormous difference. Add to those a policy of releasing all software developed by or for the Commonwealth under FOSS licences (and just as importantly, assigning resources to help nurture & build the external development communities around those projects) and you'll have a game-changing formula for success. See also our comments in Section 4.1.

> *2. Has there been a time that you tried to provide innovative ICT solutions to the Australian Government and failed? Please provide examples about what happened, and what you think the impact was.*

For obvious reasons, each company contributing to this paper must answer this question separately.

Safecoms Cyber Security is a new start-up company. Our first productised services are scheduled for launch later this year. At present our live market offerings consist solely of information security consulting. Since our relatively recent foundation, we have not been aware of any relevant RFTs being released by the Commonwealth. So our answer is "no".

Saosce has never undertaken any projects for the Commonwealth Government either, although we have undertaken projects for various State Government agencies and LGAs. To be frank, as an SME we did not think we would satisfy the non-technical requirements for responding to Commonwealth Government RFTs.

Holden Dynamics has never contracted directly to the Commonwealth. However, Holden Dynamics has delivered parts of Commonwealth Government projects in the past (specifically, for the Department of Defence), as a subcontractor to various larger prime contractors.

Those projects have all been successful. It is difficult to comment on the procurement process in those cases, as direct engagement in the procurement process is always the responsibility of the prime contractor, not its subcontractors.

Anecdotally however, the most common issue seemed to be rigid thinking in the agency: an unwillingness to consider novel or innovative approaches & ideas, preferring instead to order another iteration of the "tried & true" approach in each case.

3 Snapshot of ICT procurement

3.1 Contract size & industry perceptions

We were interested and somewhat surprised to read in the discussion paper that the Commonwealth Government's median ICT contract value was only $55,000. This is not widely known in industry. Perhaps if it were, more SMEs may bid on Commonwealth Government contracts.

This mismatch between industry's perception of the size of contract the Commonwealth tends to award and the actual figures may well explain in part the excessive use of a small cadre of large vendors, as documented in the paper: if most SMEs expect Commonwealth projects to be of a scale beyond their capability to deliver, it is not surprising that most SMEs do not respond to Commonwealth RFTs. Likewise if the agencies receive responses mostly from those large vendors, it is hardly surprising that those vendors often end up prevailing.

3.2 SME involvement

We fervently agree with the discussion paper's assertion (on p. 4) that "[i]ncreasing SME involvement is one way to drive greater innovation in government service delivery. Removing barriers, lowering costs and streamlining procurement processes will allow more SMEs to compete for government work".

In general terms, SMEs tend to be more agile—and hence more likely to innovate—than their larger brethren. Established incumbents also have little incentive to innovate in comparison to newer entrants to the public procurement marketplace.

It is disappointing that the Commonwealth appears to be "locked in" to the largest vendors and as yet has no whole-of-government strategy to transition out of that situation.

Recommendation Signal more clearly in the marketplace the Commonwealth's desire to increase greatly the proportion by value of its ICT contracts awarded to SMEs.

Of the four barriers to SME involvement which the discussion paper noted had been identified by past reviews, the third ("Unrealistic terms and conditions, particularly in relation to liability risk regimes and intellectual property") is most likely the greatest.

Whilst we have seen no evidence of the Commonwealth Government doing this, we note that at least one State Government has attempted to require suppliers of FOSS to provide IP indemnities (with unlimited liability attached!), whilst *not* requiring any such guarantee from suppliers of equivalent closed source software. Such practices suggest a rather naive misunderstanding of the nature of the software development process and of software licensing in general: whilst there is *some* risk of malicious contribution of infringing third-party code to FOSS projects, that same risk is orders of magnitude greater in closed source software, since by definition its code base cannot have been scrutinised by large numbers of independent developers (and therefore any such aberrations in closed source software are likely to go unnoticed for far longer, amplifying the associated risk).

It is also worth noting that the financial viability requirements are clearly geared to the legacy/ closed source software development model. When procuring closed source software, it is indeed essential to ensure that the supplier is of a size & longevity and in circumstances which suggest it is highly likely to survive well beyond the planned lifecycle of the software being deployed. That is the case because with closed source software, the software vendor is the only entity capable of maintaining the software (since nobody else has the source code). The risk of the software becoming orphaned carries extreme consequences, so it is understandable that the Commonwealth seeks to protect itself from that risk. Even where escrow agreements are used, without the supporting technical documentation and the vast array of corporate memory that is lost when a closed source vendor goes under, at the end of the day the source code retrieved from escrow may well be effectively unmaintainable.

By contrast, with open source software *any* competent programmer is capable of maintaining the software.

This does not mean that the Commonwealth should cease assessing suppliers' financial viability. But it does mean that for suppliers of open source software the bar can be set somewhat lower quite safely. It is still important to ensure that the supplier is highly likely to survive to—and at least a little beyond—project completion. Thereafter, who maintains the software is a question unrelated to the original project.

In fact, one of the great benefits of open source software is the secondary market for software maintenance & support, the competition in which tends to drive down costs. Government may well wish to consider approaching the market for maintenance & support quite separately from the original approach for design, integration, etc..

Recommendation Lower the supplier financial viability criteria substantially for any contract in which the supplier guarantees that all software supplied will be licenced to the Commonwealth under terms which comply with the Free Software Definition and/or the Open Source Definition.

3.3 Response to specific questions

> *3. In what areas of the Australian Government's ICT procurement are the biggest opportunities for innovative technologies?*

To date, most ICT innovation in the Commonwealth Government has occurred around the web. By and large this has been good work, which should be welcomed.

However, as a result the biggest opportunities for innovation in the Commonwealth ICT today lie in other software domains, beyond the web.

Infrastructure software like mail systems & database management systems, accounting & enterprise resource planning (ERP) software and desktop software (both applications software and operating systems) are all obvious candidates. We are not at all surprised that some of those areas where little if any innovation has occurred to date also appear amongst the greatest areas of spend in the chart on page 3 of the discussion paper.

It also worth noting that one of the findings of the Commission of Audit was the excessive number of disparate, incompatible deployments of *the same* ERP system (SAP) found deployed across government. Such areas are ripe for change.

Recommendation Focus on seeking novel & innovative solutions in those areas in which the least innovation has occurred in recent times and which also account for the lion's share of Commonwealth ICT spend.

> *4. What are the key barriers to getting innovative technologies, such as cloud services, into the Australian Government?*

The key barrier to getting innovative technologies into the Australian Government appears to be a lack of flexibility. Agencies need to be willing to *consider* novel & innovative approaches with an open mind.

The question specifically mentions cloud services. "The cloud" is somewhat of a double-edged sword. Naturally the biggest barrier to adoption of cloud services in *any* organisation is the need for information security. That however is a legitimate barrier, not an artificial one.

In our view, governments should *never* allow any confidential data on its citizens to walk out the door. This proposition is not incompatible with the idea of cloud services in general, although it is incompatible with the vast majority of cloud services offered today.

It *is* possible to realise the benefits of cloud services whilst preserving acceptably high levels of information security—only by subjecting all data to be stored "in the cloud" to strong encryption (for which the service provider must *not* have the keys) *before* it leaves the agency.

Such services do exist (although today they are still few and far between) and indeed Safecoms will be launching one such cloud service this year.

Naturally, for such a service to be trusted, any client-side software it requires *must* be released under a FOSS licence, as otherwise it is impossible to verify if, where & how the claimed encryption occurs.

Finally, we see it as imperative that the infrastructure on which any cloud service to be trusted by government resides be physically located on Australian soil. Conflict of privacy laws in different jurisdictions and other data sovereignty risks are simply too grave to ignore.

We understand that Australia is party to a number of international treaties which prohibit local preference in public procurement. Whilst those treaties often contain exceptions for certain areas, those exceptions are far too narrow. We welcome the Treasurer's recent statement that the Commonwealth will pursue an "Australia first" trade policy[15] and we hope that that means that Australia will follow the latest global trend, both by re-negotiating those existing treaties that have been disadvantageous to Australia (including all those which prohibit local preference in public procurement) and by pursuing new *genuine* free trade agreements (i.e. those which focus solely on reciprocal elimination of tariffs & quotas, to the exclusion of all else).

Recommendation Establish a policy of never ratifying or acceding to any treaty which prohibits local preference in public procurement and renegotiate all such existing treaties without the offending provisions.

> *5. What are the key barriers for SMEs and startups in the Australian Government's ICT procurement process?*

In our view, the six key barriers to SME & start-up participation in public procurement are as follows:

- Excessive financial viability criteria (see also Section 3.2);
- Entrenched institutional bias in favour of a small cadre of large vendors (see also Section 6.1);
- Unwillingness to consider truly novel & innovative ideas or approaches;
- Approaches to market for specific products or specific classes of products, rather than for any demonstrably valid solution to the agency's specific business requirements;
- Ill-considered treaties which prohibit government from reinstituting sensible policies for local preference; and
- Fear of "open source risk" without much (or sometimes any) understanding of the equivalent (and far greater) "closed source risk" (see also Section 3.2).

4 Rules

4.1 Open source software policy

There is a strong link between procurement of open source software (OSS) and digital transformation[16], an opportunity missed by successive Australian governments. The Australian Government Open Source Software Policy[17] lacks commitment and direction. Compared with the US, the UK & the EU, the Australian Government has been very timid in its support and direction for the use of open source software, as the extracts below demonstrate.

For example, in the United States, since 2016 the Federal Source Code Policy[18] has required Federal agencies to release at least 20 percent of newly commissioned custom software under open source licences, in order to: encourge greater reuse by agencies; drive competition among vendors for maintenance & enhancement work by ensuring they have full knowledge of the underlying code; and encourage innovation among software developers who look to adopt and adapt the code for innovative new services.

[15] Weinstein, A., *'Australia First' Policy Embraces Trade, Treasurer Morrison Says*, Bloomberg Markets, 25 Jan 2017. Available at https://www.bloomberg.com/news/articles/2017-01-24/-australia-first-policy-embraces-trade-treasurer-morrison-says.

[16] Backaitis, V., *How Open Source Guides Digital Transformation*, CMS Wire, 18 July 2016. Available at: http://www.cmswire.com/digital-experience/how-open-source-guides-digital-transformation/

[17] https://www.finance.gov.au/sites/default/files/australian-government-open-source-software-policy-2013.pdf

[18] https://sourcecode.cio.gov/

It should be noted that the only component of the much maligned `HealthCare.gov` initiative that did *not* fail was built entirely on open source code by a start-up called Development Seed[19]. The code is publicly available on Github.

In the United Kingdom, Her Majesty's Government has long had an active role in promoting the adoption of OSS. Their early adoption (2002, updated in 2012) of an open source software policy effectively laid the foundations for the Government Digital Service[20] and the Digital Service Standard[21] by putting open source adoption at the heart of their digital reforms[22]. The key points of the UK OSS policy are:

1. The Government will actively and fairly cosider open soruce solutions alongside proprietary ones in making procurement decisions.

2. Procurement decisions will be made on the basis of the best value for money solution to the business requirement, taking account of total lifetime cost of ownership of the solution, including exit and transition costs, after ensuring that solutions fulfil minimum and essential capability, security, scalability, transferability, support and manageability requirements. Where a 'perpetual licence' has previously been purchased from a proprietary vendor (and therefore often giving the appearance of a zero cost to a project), a shadow licence cost shall be applied to ensure a fair comparison of total cost of ownership. The shadow licence cost will be equivalent to the published list price of the product (no discounts can be factored in), or the price the public sector pays overall on a 'crown' deal.

3. The Government will expect those putting forward IT solutions to develop where necessary a suitable mix of open source and proprietary products to ensure that the best possible overall solution can be considered. Vendors will be required to provide evidence of this during a procurement exercise. Where no evidence exists in a bid that full consideration has been given to open source products, the bid will be considered non compliant and is likely to be removed from the tender process.

4. Where there is no significant overall cost difference between open and non-open source products, open source will be selected on the basis of its additional inherent flexibility[23].

Point 2 reflects the cost competitiveness of OSS over closed source solutions when taking into account the total lifetime costs of ownership (including exit migration costs—see Section 4.2).

Similarly, in 2012 France issued a guideline favouring FOSS in the public administration, which required agencies to make "a systematic review of free alternatives when doing development and major revisions of applications" and recommended that agencies build up FOSS expertise & contribute code back upstream[24].

In 2016, Bulgaria went even further, passing the *Electronic Governance Act 2016 (Bulgaria)*, which provides (at Art. 58) that:

> "When the subject of the contract includes the development of computer programs, computer programs must meet the criteria for open-source software; all copyright and related rights on the relevant computer programs, their source code, the design of interfaces, and databases which are subject to the order should arise for the principal in full, without limitations in the use, modification, and distribution; and development should be done in the repository maintained by the agency in accordance with Art 7c pt. 18."[25]

Similarly, Vietnam has mandated that *all* software used in government be open source[26].

A 2006 report by Novell found that "[g]overnment agencies that use open source report average savings of 40 percent to 50 percent on hardware expenses while software costs are being driven down by as much as 40

[19] https://developmentseed.org/projects/healthcare-gov/

[20] https://www.gov.uk/government/organisations/government-digital-service

[21] https://www.gov.uk/service-manual/service-standard

[22] http://www.publicsectorexecutive.com/Public-Sector-News/open-source-software-finds-its-sweet-spot-in-the-p

[23] Cabinet Office & Home Office, *ibid., p. 23*

[24] https://joinup.ec.europa.eu/news/french-guideline-favours-use-free-and-open-source

[25] Chadwick, J., *Bulgaria passes law requiring government software to be open source*, ZDNet, 5 Jul 2016. Available at: http://www.zdnet.com/article/bulgaria-passes-law-requiring-government-software-to-be-open-source/

[26] Orion, E., *Vietnamese government mandates Open Source*, The Inquirer, 8 Jan 2009. Available at: http://www.theinquirer.net/inquirer/news/1050293/vietnamese-government-mandates-open-source

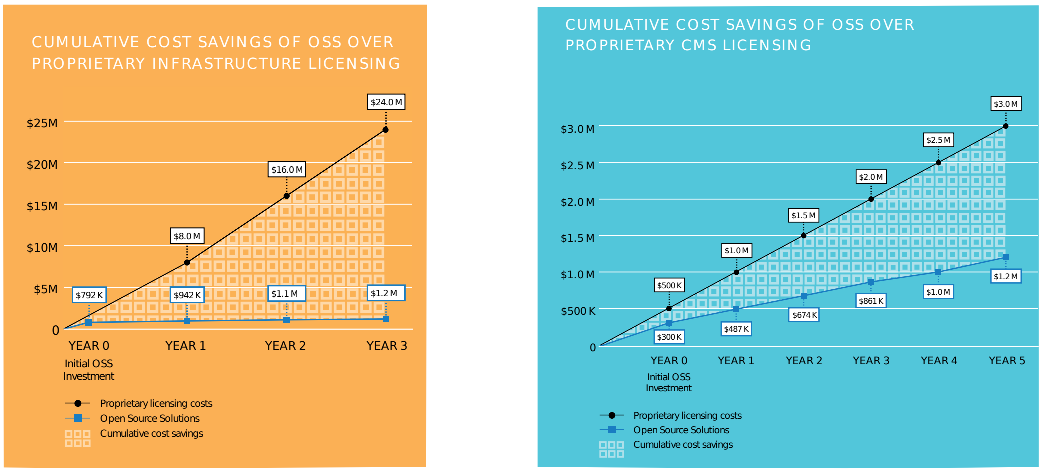

Figure 1: Cumulative cost savings of OSS over closed source in two case studies (source: OCI, 2015, pp. 6–7.)

percent"[27]. More recently, a report by OCI in 2015[28] underscored the whole of life cost savings available to government, as shown in Figure 1.

The US, UK & EU approaches stand in stark contrast to the three Principles of the Australian Government Open Source Software Policy, which are:

1. Australian Government ICT procurement processes must actively and fairly consider all types of available software.
2. Suppliers must consider all types of available software when dealing with Australian Government agencies.
3. Australian Government agencies will actively participate in open source software communities and contribute back where appropriate.

Those policy principles provide very little whole of government leadership to agencies and little or no reassurance to the FOSS sector in industry that they will be treated equally (let alone preferentially) in procurement activities.

Perhaps as a result, the adoption of FOSS by the Commonwealth appears to have been centred around web sites and content management systems but has not penetrated much further into the software stack, as has happened in other jurisdictions.

We say "appears" because there is no authoritative data available publicly. Perhaps industry would be better equipped to advise on these matters if the Commonwealth were to publish performance data on the uptake of FOSS across APS.

Recommendation Overhaul its Open Source Software policy, at the very least to bring it into line with the rest of the world, ideally to place Australia in a world-leading position. Ideally the revised policy should include:

(a) a firm preference for open source software, coupled with a requirement for detailed justification & external review before an agency may procure software under any licence that fails to grant the rights of modification & redistribution; and

(b) a requirement that all non-classified software developed by or for the Commonwealth be released publicly under licenses compliant with the Free Software Definition and/or the Open Source Definition.

[27] *Open Source Special Report: Separating Fact From Fiction*, Novell, 2006, p. 2. Available at: http://icma.org/Documents/Document/Document/301454

[28] *A Guide to Open Source Transformation Services: How and Why Organisations are Making the Move to Open Source*, OCI, 2015. Available at: https://www.ociweb.com/files/2314/4837/7674/OSTS_web_v3_1.pdf

4.2 Migration costs

The Commonwealth Procurement Rules (CPRs) require taking into account "whole-of-life" costs[29], which is as it should be. Migration costs are often amongst the greatest cost components of large ICT projects.

However, migration costs are being considered at the wrong time. A sensible evaluation of a project proposal would consider its *exit* migration costs, not its *entry* migration costs. Whilst the CPRs require[30] the consideration of "transition out costs" (exit migration costs), anecdotal evidence suggests that agencies often consider entry migration costs instead—in other words, Rule 4.6(f) is not always being enforced.

In most cases, software is being procured to replace existing software. The cost of migrating from one implementation to the next is a function of the manner in which the *incumbent* project was designed & implemented, not a function of its successor.

Excessive exit migration cost is one of the principal tools used by nefarious suppliers to perpetuate vendor lock-in. So evaluating entry (instead of exit) migration costs creates a disincentive to breaking vendor lock-in and a disincentive to innovation in general.

The glaring nature of this financial modelling error is most evident when one considers green-fields projects. By definition, they have no entry migration costs, only exit migration costs. If the evaluation fails to consider exit migration costs, that *encourages* bidders on green-fields projects to attempt vendor lock-in. Conversely, if the consideration of exit migration costs were to be enforced consistently, that would encourage bidders to propose solutions that will help reduce the Commonwealth's long-term spend.

It should be noted that in the United Kingdom, Her Majesty's Government has required procurement decisions to take exit migration costs into account for some years now[31] and that change has delivered both long-term cost savings for HMG and acceleration of its digital transformation agenda.

The best way to limit migration costs—in addition to requiring exit migration costs to be taken into account in the initial evaluation—is to mandate that all data formats (whether for data interchange or for local storage) and all communication protocols conform to unencumbered open standards.

Recommendation Enforce consideration of *exit* migration costs in the evaluation of all ICT proposals & tenders.

Recommendation Prohibit the procurement of any software which fails to adhere to the relevant unencumbered open standards for all data storage & communication.

4.3 Agency-specific rules

The existence of agency-specific rules is perfectly appropriate. It is only natural that business needs and risk appetites will vary as between different agencies.

However, it is of great concern that, as the discussion paper pointed out (at p. 8), "[t]hese rules may not be publicly available".

Failing to publish the complete set of procurement rules applicable to any given project creates an inherent bias in favour of incumbent suppliers, who are already aware of the rules. How are new entrants to the public procurement marketplace expected to propose optimal solutions when they are kept in the dark as to the rules against which those proposals will be evaluated?

Recommendation Make all agency-specific procurement rules publicly available.

[29] Rule 4.5(f).

[30] Rule 4.6(f).

[31] Cabinet Office & Home Office, *All about Open Source: An Introduction to Open Source Software for Government IT*, version 2.0, Her Majesty's Government, April 2012, p. 8, point 2. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78959/All_About_Open_Source_v2_0.pdf

4.4 Model contracts

Model contracts are a good idea in theory. Indeed, in many procurement domains outside of ICT, they may be highly effective. However, a model contract is not much help when software vendors are still allowed to dictate the terms of the licenses under which the agency acquires the software.

To be effective for ICT procurement, any model contract should specify a *minimum* set of rights which the agency must acquire under any software licence.

We believe that a suitable minimum set of rights would be: the right to use the software for any purpose; the right to inspect its source code; the right to modify it; and the right to redistribute it (either verbatim or modified).

It is no accident that those rights correspond closely to the freedoms laid out in the Free Software Definition[32] and to the first three of the ten criteria in the Open Source Definition[33]. Those rights, and the freedoms they confer, should be seen as just as important to Commonwealth agencies as to any other end user or end user organisation.

See also our comments in Sections 2.1 & 4.1 and Recommendations 1 & 9a.

4.5 Digital Marketplace

We commend the Commonwealth on its recent implementation of the Digital Marketplace. That initiative certainly has the potential to facilitate interaction between agencies and industry, although to be effective naturally it will need to be expanded to cover a much broader range of suppliers & services.

4.6 Response to specific questions

> *6. Are the Australian Government's ICT procurement rules easily accessible, easy to understand and navigate?*

Yes. The Commonwealth Procurement Rules are publicly available, as they should be. They are also significantly easier to digest and interpret than their counterparts published by certain State/Territory governments.

> *7. How could the Australian Government's procurement rules and processes be improved to make it easier to offer innovative solutions to government?*

The Commonwealth Procurement Rules already require that technical requirements be stated in generic terms[34]. We see that as a very good measure to prevent prejudicial specifications. However, that rule is often not enforced, which we see as a serious issue. RFTs that specify a particular technical *solution*, rather than generic technical *requirements* actively stifle innovation. That practice should be stamped out.

Ideally, agencies should go one step further. If, rather than specifying *technical* requirements, agencies were to specify their *business* requirements, there would be far greater scope for suppliers to propose a range of truly novel & innovative solutions. See Recommendation 3.

Agencies should assiduously avoid procuring software under closed source licences. Use of software obtained under licences that prohibit modification & redistribution actively stifles innovation. Use of software obtained under licences that do not guarantee access to the source code also effectively prevents agencies from implementing information security assurance measures such as code audits[35]. In our opinion, both of those risks are too great for any agency to consider continuing to accept. See Recommendation 9a.

Finally, the Commonwealth would be well advised to renegotiate all relevant treaties to remove prohibitions on local preference in public procurement, then amend the Commonwealth Procurement Rules to reinstate local preference. See Recommendation 8.

[32] Stallman, *op. cit.*

[33] Perens, *op. cit.*

[34] Rules 10.9 & 10.10.

[35] Whilst the *Copyright Act 1968 (Cth)* does contain an exception (s. 47F) for investigating & correcting security vulnerabilities, the utility of that exception is limited, since decompiled object code is far more labour intensive to analyse than original source code. In addition, certain vendors' use of "Technological Protection Measures" (TPMs) may render the object code effectively unmodifiable.

> *8. What rules, including any security requirements, limit the Australian Government's use of cloud services?*

It is true that security requirements currently limit agencies' use of cloud services. However, that is not the fault of the security requirements (which in most cases are appropriate). Rather, it is a result of most (but not all) cloud services currently on offer being fundamentally incompatible with sensible security requirements.

The solution lies: firstly in careful selection of which cloud services agencies should consider using; and secondly in abandoning the present "cloud first" strategy and substituting a "fit for purpose" strategy under which proposed cloud & on-premise solutions are each evaluated on their merits for the specific project.

Naturally, industry has a role to play too, in increasing the number of genuinely secure cloud services on offer. One of Safecoms' divisions is dedicated to doing just that and a few others in the industry are also starting to go down that path, but unfortunately the vast majority of cloud services in the market today pay little more than lip service (if that) to their clients' information security needs. A strong message from government that security is a paramount requirement when evaluating cloud services might help bring more of the industry on board.

Finally, we firmly believe that no Australian government data should ever physically reside overseas. Whilst rigid prohibitions on local preference remain in place, it is difficult for government to consider any cloud services, given the data sovereignty risks. Steps should be taken to enable the removal of those prohibitions.

See also Section 3.3.

5 Capability

5.1 Responsibility for procurement

The discussion paper states (at p. 9) that "[p]rocurement in government is generally undertaken by procurement officers based within individual agencies and requires a range of capabilities". The accompanying figure outlined a range of required capabilities, all of which are generic procurement capabilities.

That is a big problem. What's missing from the picture is current domain-specific expertise, which is by far the most important capability for anyone responsible for complex or large-scale procurement.

Whether to place greater emphasis on the need for generic procurement skills or on the need for domain-specific expertise is an age old question in procurement. Clearly the Commonwealth has opted for the former, whilst industry (or at least, the honest & competent players in the industry) would would have preferred the latter.

But such a dichotomy does not have to exist. It is feasible (and indeed preferable), at least for large or complex ICT procurements to be undertaken by a suitably constituted committee, ideally consisting of: at least one procurement professional (to ensure that all procurement rules and processes are adhered to); at least one representative of the intended end user base (to ensure that the selected solution is indeed fit for purpose); and at least one indepedent computing professional with deep, relevant domain-specific expertise (to ensure that the best solution is selected).

The latter need not even be drawn from within government, although if drawn from industry, naturally strict rules to avoid conflicts of interest would be necessary.

5.2 Collaboration

The discussion paper goes on to point out "[w]hile collaboration is often espoused as an objective of government in ICT procurement it can be difficult to achieve in practice, especially in the context of procurement rules and probity requirements". Whilst that is true, we can see a number of potential paths to ameliorating that difficulty.

One possibility is strict enforcement of the separation between trusted advisers and implementers. "Chinese walls" can be dangerous and should not be trusted: under this approach, accepting a contract as a trusted adviser would irrevocably disqualify the supplier, all the supplier's staff and any related entities from bidding on the implementation, or being involved in any other way (e.g. as a subcontractor) in the implementation.

An alternative would be to engage in the sort of collaboration for which open source software projects are best known: a totally transparent, public process. Whilst that might not always be feasible for some government projects, no doubt there will be others for which it is.

For those where it isn't, we propose at least a partial opening up of the pre-procurement (trusted adviser) phase, in order to foster greater innovation. This is the competitive consulting process we wrote of in Section 2.2, which we could envisage working as follows.

When a large, complex or unique (but unclassified) business requirement arises at an agency, *first* approach the market with an EOI for developing a strategy to address the requirement. So far, no different to any other consulting arrangement. The difference comes next.

Instead of engaging a single preferred consulting firm, engage a range (say, perhaps six) of them, on the basis of the quality of the EOI responses received. Each selected firm would work independently in parallel on their own strategy, competing with each other to develop the best model selected by the agency. In order to ensure equitable competition, upon delivery of their final reports each firm should be paid the same fixed fee, determined by the agency based on the scale of the business requirement (and published in the EOI, so that all respondents know in advance what they're getting themselves in for). Perhaps an additional amount should be payable to the firm (if any) whose model is selected, as a further incentive to innovation. Naturally, it should be a strict requirement that all recommendations must be made in generic terms, suitable for use in an unbiased procurement exercise for the implementation.

At the conclusion of that process, the agency could run a standard procurement process for implementation of the selected solution. Because the business analysis would have been conducted competitively, in the open, any potential conflict of interest issues would be moot, so there would no longer be a strong need to prohibit the firms who participated in the consulting procurement from participating in the implementation procurement.

We acknowledge that such a process requires far more mature capabilities & culture in the acquiring agency than traditional procurement processes do. Nevertheless, if implemented well, a process like that could result in a massive increase to innovation in government ICT.

We acknowledge also that there are new costs associated with the competitive consulting phase of that process. However, those costs will be offset by cost savings from the more innovative approaches that will inevitably result. It seems likely (although not certain) that, at least on large, complex or unique projects, the savings would substantially outweigh the costs.

5.3 Response to specific questions

> *9. What capabilities does the Australian Government need to be able to take full advantage of digital technologies, now and in the future?*

Deep domain-specific expertise needs to be at the very core of the procurement process. See our comments in Section 5.1.

In addition, agencies need to think outside the square. To achieve major increases in innovation in government ICT, first it is necessary to adopt novel & innovative approaches to ICT procurement which are designed from the ground up to foster innovation. See our comments in Section 5.2.

> *10. In your exeperience, what are the biggest capability gaps in Australian Government ICT procurement? How could the Government better develop or access the capability required?*

Again, more domain-specific expertise is required in ICT procurement. That could be achieved through new hires, or equally by appointing independent consultants to suitably constituted procurement committees on short-term contracts.

In Section 2.1 we wrote of the need to substitute a range of more flexible acquisition models for the traditional "buy versus build" decision. In the context of software procurement, that requires personnel with a good appreciation of open source software development methodologies.

In addition, approaching the market far earlier in the process is likely to be highly beneficial. For some ideas on how that might be accomplished, see our comments in Sections 2.2 & 5.2.

> *11. In your experience, has the governance approach used by agencies to manage large ICT projects enabled or inhibited the success of those projects?*

The authors of this paper have no direct experience of the governance processes used by Commonwealth agencies when managing large ICT projects. Therefore, we can only offer our views here generically, in the context of a few major Commonwealth ICT projects which been subject to great public scrutiny (after the fact) in recent times.

Firstly, it is important for agencies to realise that outsourcing, whilst a very useful tool, does not relieve them of responsibility. The 2016 census provides a textbook example of why.

It is also vital that selected architectures are arrived at by a thorough, reasoned, analytical and completely transparent process. Government has done that for many years when designing & evaluating complex public policy initiatives, but often overlooks the need when it comes to designing & evaluating complex ICT systems. The recent, widely publicised storage incident at ATO (where a fatal error in the production SAN propagated automatically to the backup SAN) is a case in point.

Finally, the importance of risk management cannot be understated. Although we are of course great supporters of novel & innovative approaches in computing, it is well worth noting that when an approach is *exceedingly* novel or innovative and *also* has direct impact on citizens, as a sanity check it is often worth undertaking suitably comprehensive independent technical, legal & ethical reviews at the outset and again at various points as the project matures. The recent issues that have arisen from the Centrelink automated debt recovery initiative (a novel application of artificial intelligence & other statistical modelling to one field which by its very nature is better suited to more precise methods) provides a clear example of the sort of project on which such reviews should form a key element of the risk management strategy.

A greater emphasis on the necessary governance processes might help reduce the frequency of such technical, policy and public relations disasters in future.

It is perhaps also worth noting that when things do go awry in a software development project (although not necessarily other classes of computing project), being able to refer to a commit log[36] that is publicly available (as is the case in almost all FOSS projects) may help to avoid the sort of wild speculation as to questions of accountability sometimes seen in the media in the aftermath.

6 Culture

"Having the right culture in government is crticial" was the first sentence of the discussion paper's section on culture. We couldn't agree more. The same is true in industry and indeed in the not-for-profit sector. As Peter Drucker once said, "culture eats strategy for breakfast".

Whilst it is easy to recognise the benefits of having "the right" culture (and indeed the detriment of having a dysfunctional culture), actually achieving cultural change is rather more difficult, for any organisation (government or otherwise).

Nevertheless we applaud the task force's decision to place great emphasis on the importance of organisational culture in fostering innovation.

[36] It is considered best practice in software development to use a revision control system (e.g. *CVS*, *Subversion* or *Git*) to manage the source code. Such systems track exactly what code was changed (or added or removed), when and by whom. Each such change made to the code base is called a "commit". Each commit has a brief message associated with it, summarising the change & its purpose. In a well-governed project, each commit message will also note who *approved* the change (in large, complex projects another best practice is for each change to be reviewed by a developer other than the one proposing it before committing the change). A commit log is just a list of commits in chronological order, showing for each commit its commit message, which file(s) were affected, who committed it and when. In closed source developement, revision control systems (and therefore the commit logs they can produce) are generally accessible only within the developing organisation. In publicly maintained FOSS projects, whilst obviously only the project's core developers (for that reason often called its "committers") can commit changes, read-only access to the revision control system (which is all that is required to generate commit logs) is usually granted to the general public.

6.1 Inertia, bias & anticompetitive procurement: a case study

In any large organisation (not just in government) there tends to be a certain inertia—a bias toward the familiar. The Commonwealth's Microsoft Volume Sourcing Arrangement[37] (MVSA) is a case in point, where the pull to the familiar appears to have trumped all reason. The MVSA is completely out of step with contemporary approaches taken in the rest of the world.

Whilst the MVSA might have delivered some cost savings over its predecessor, it has effectively excluded Australian software development & integration companies from offering FOSS desktop (and to a lesser extent mobile, server & cloud) solutions to the Commonwealth and by doing so served as a major disincentive to innovation, particularly for Australian SMEs.

The very existence of the MVSA also appears to violate the spirit (and perhaps even the letter) of the Commonwealth Procurement Rules. Was this arrangement ever put out to open tender? If not, why not? For such a major element of the Commonwealth's ICT procurement to bypass the standard competitive processes casts serious doubt on the Commonwealth's commitment to those processes. This is altogether the wrong message to be sending to industry, if the Commonwealth is serious about innovation in public sector ICT.

We call upon the Commonwealth to release publicly details of how the MVSA was negotiated, what savings (if any) it has achieved to date and how those savings were calculated.

In practice, The MVSA locks FOSS desktop (and again, to a lesser extent mobile, server & cloud) solutions and the innovative Australian SMEs who develop & support them out of a large chunk of Commonwealth business. It sends the message to competitors that in those very broad areas of ICT the Commonwealth is a closed shop.

The situation is somewhat different in the United Kingdom and in Europe. For example:

In the UK, the Crown Commercial Service has entered into an agreement on behalf of public sector organisations to provide an open source office productivity suite (Collabora GovOffice, based on The Document Foundation's LibreOffice[38] on the basis of "considerable cost savings compared to competing pacakges"[39].

Similarly, the Netherlands Parliament is set to introduce a law in 2017 mandating the use of open document formats in public administration[40].

In the UK, Barclays Bank is claiming 90% cost savings on software by moving to an internal private cloud environment using open source GNU/Linux software[41]. Although Barclays is a private sector organisation, their operations are of a similar scale to many public sector organisations which could no doubt achieve similar savings, were the path to innovation not blocked in Australia by the MVSA.

In France, the Gendarmerie Nationale reported 40% cost savings from migrating to open source software (GNU/Linux & OpenOffice) on 65,000 desktop computers[42].

Also in France, the City of Nantes reported up front cost savings of EUR 1.6M plus steady-state cost savings of EUR 260,000 per annum just from having switched 5,000 desktop users from Microsoft Office to LibreOffice[43]. Very sensibly, Nantes have allocated 11% of their steady-state savings from this initiative to investing in further development of LibreOffice and contributing their changes back upstream.

In 2016, the Lithuanian police force reported EUR 1M savings from switching 8,000 workstations from Microsoft Windows & Office to GNU/Linux & LibreOffice[44].

The Italian military migrated its first 8,000 workstations to LibreOffice in 2016 and plan to migrate the rest of its 100,000 workstations within four years, which is estimated to yield savings in the range EUR 26M–29M.

[37] See http://www.finance.gov.au/policy-guides-procurement/mvsa/

[38] http://www.libreoffice.org/

[39] Crown Commercial Service, *Collabora deal will provide savings on Open Source office software*, Her Majesty's Government, 20 Oct 2015. Available at: https://www.gov.uk/government/news/collabora-deal-will-provide-savings-on-open-source-office-software

[40] Hillenius, G., *NL Parliament makes open standards mandatory*, European Commission, 12 Oct 2016. Available at: https://joinup.ec.europa.eu/community/osor/news/nl-parliament-makes-open-standards-mandatory

[41] Worth, D., *Barclays claims 90 percent software cost savings with open source drive*, V3, 9 Jan 2013. Available at: http://www.v3.co.uk/v3-uk/news/2234593/barclays-slashes-software-spend-by-90-percent-with-open-source-drive

[42] https://joinup.ec.europa.eu/community/osor/news/open-standards-and-itil-lead-open-source-frances-gendarmer

[43] https://joinup.ec.europa.eu/community/osor/news/nantes-open-source-cuts-recurring-charges

[44] https://joinup.ec.europa.eu/community/osor/news/lithuanian-police-switched-libreoffice

Recommendation Use genuinely competitive processes for procuring all desktop software (and all other classes of software currently covered by the MVSA).

6.2 Response to specific questions

> *12. How does culture influence the Australian Government's approach to ICT procurement? What sort of culture change would better support innovative ICT services and get more SME and startups working with the Government?*

Whilst it is no doubt true that the present culture is risk-averse, that in itself is not a problem—one expects governments to be risk-averse. Rather, the problem is how thoroughly one analyses risk.

Perpetuating the status quo can often be a riskier proposition than taking a new, innovative approach that wasn't available the last time the question was raised.

However, as noted in Section 6.1, large organisations tend to exhibit inertia: a bias toward the familiar. This is not risk aversion, it is an aversion to critical thinking. The genuinely risk-averse would naturally apply the same rigorous analysis to the risks associated with the ubiquitous "do nothing" option as to those associated with novel & innovative models. Again, government has long taken that approach when analysing models for regulatory reform; it is essential that the same approach is applied to analysing models for ICT change.

Cultural change is difficult to achieve at the best of times. It will probably be particularly tricky to eradicate the inertia/bias described above *without* reducing the healthy level of genuine risk-aversion.

The major cultural shift required in public procurement is to move away from seeking *products* and towards seeking innovative approaches & solutions to the actual business problems faced by agencies.

See also our comments in Section 6.1.

> *13. What exeperience have you had with 'partnering' with the Australian Government and what is required to do it better?*

As a recent start-up, Safecoms has not "partnered" with the Commonwealth Government to date.

However, Safecoms looks forward to doing so (as do Holden Dynamics & Saosce), when suitable opportunities next arise, including but not limited to advising on the implementation of any of the initiatives proposed in this document.