Australian Commission of Audit. 29/011/2013

Thank you for the opportunity to submit into your process.

Our company develops software for the Australian and International markets, our intention is not to promote commercial interest in this submission but to share particular insights.

Three main process challenges exist for both the Government and Private Sector in Australia.

They are:

1) **Architecture.**

(a) It doesn't optimize the collection of most relevant data, limits the quality and currency of decisions and throws up barriers to execution everywhere.

Digital flexibility and related public interest process is constrained.

b) Reinforces silo and territorial barriers both within Government and between the three levels of Government.

c) Pushes back on improvement change by adding significant risk to major projects and cost.
Non-delivery then becomes a political management challenge, all at the expense of the public interest and front line service delivery.

2) **Leveraging from a 'Whole Government Cloud'.**
a) Lack of appreciation <u>to not use</u> 'cloud' is a discretion, which <u>economics will not permit in the future</u>. The cloud cost saving and continued cost reduction of between 30% to 70% will be compelling.
b) Having geographical limits on the location of cloud infrastructure and confining to state boundaries is reminiscent of the multiple incompatible state railway gauges of the past. Thoughtless waste.
c) There should be one separate, exclusive to "Whole of Government" Cloud infrastructure operated by a tier one private sector provider which all governments in Australia resource from.   Federal/State and Local.

3) **Security.**
a) <u>It is everything.</u> As per Melissa Hathaway (from CISCO USA) sentiment expressed when visiting Australia in November 2013 "Cyber Security is not an "after thought", an " add on" or a matter for statements of "correctness".
Cyber Security is everything. It is the primary determinant for the success of every process and result. (Refer to Cyber Maryland statement by the State Government of Maryland in the USA)< http://issuu.com/cybermaryland/docs/cyberreport>

<http://www.youtube.com/watch?v=bA_NEe3GBZQ>

b) <u>We have got used to all being directly connected.</u> Existing architecture is challenged by direct connection. Hacking, loss of IP , breach of privacy and theft of data is endless. Even with firewall based partitioning the direct connection structure of the Internet and everyone's appliances and systems gives attackers and thieves in many cases reliable predictable access almost at their discretion.

c) Stronger security tends to be at the expense of organization/user functionality. And vice a versa. Meeting more user/org demands trades away and weakens security. This is a fundamental barrier to optimum process synergy in government.

Solution for the problems of architecture, leveraging cloud and security.

1) Create a new type of neutral network to integrate, secure and drive the productivity improvements demanded of efficient Gov. process.

This independent network would facilitate virtual integration of any Gov. system, user or database without the need to change existing investments in IT.

This network has capability to configure and connect any system, network or technology. And in any number.

By developing an independent stand alone network which places itself out in front of Gov. systems, networks, servers and appliances, Government will be able to remove itself from direct public exposure to its info systems in front line delivery of services. This is a valuable capability when using cloud infrastructure.

2) This independent network embodies a series of separate services for email, web service, exchanging files, data extraction, mixing and reporting, remote access for employees on any device, secure administration, measurement and others. Audio, video would also be handled.

3) The independent network uses particular services to remove the public/static broadcast of IP addresses. This adds extra privacy for individuals and a new dynamic of information defense.

Conclusion.
Rather than provide extensive detail at this stage should the Commission of Audit be conducting oral hearings in Perth we would welcome the opportunity to expand further.
We would also be available by telephone to discuss various possible courses of action, which might be available to the commission through the engagement of this virtual neutral network infrastructure.
We are currently working with one the United State's Government major suppliers.

██████████

**An Officer of
IWebGate Technology Ltd**