Submission

No 10

FOLLOW UP OF THE AUDITOR-GENERAL'S PERFORMANCE AUDITS SEPTEMBER 2010 - FEBRUARY 2011

Organisation: Department of Premier and Cabinet

Name: Mr Chris Eccles

Position: Director General

Telephone: 9228 5555

Date Received:

Theme:

Summary

NSW GOVERNMENT | Premier & Cabinet

2012/13036

The Hon. Jonathon O'Dea, MP
Chair, Public Accounts Committee
Legislative Assembly
Parliament of New South Wales
Macquarie Street
Sydney, NSW 2000

Dear Mr. O'Dea

I refer to your letter to me dated 28 February 2012 regarding the Auditor-General's Report on Electronic Information Security. Please find enclosed the Department of Premier and Cabinet's response to this report. This response has been prepared in conjunction with the Department of Finance and Services, Office of ICT Strategy and with the Chair, Electronic Information Security Working Group. Please accept my apologies for the lateness of this submission.

If you have any questions regarding the submission, please contact myself or our Chief Information Officer, Emily Morgan, on telephone 9228-5815.

Yours sincerely

Chris Eccles
Director General

Cc: The Hon. Barry O'Farrell MP

PERFORMANCE AUDIT – Electronic Information Security

Implementation of Recommendations May 2012 Status

Recommendation	Accepted or Rejected	Actions to be Taken	Due Date	Status and Comment	Responsibility
1. *minimum cross-Government standards, policies and rules are established with which all agencies must comply, while recognising that individual agencies need to assess their own risk and may need to put in place a higher level of protection*	Accepted	Department of Finance and Services through the new ICT Strategy to establish an Information Security Policy for all agencies	December 2013 for implementation May 2012 for ICT Strategy	On Track ICT Strategy due for release in second quarter 2012	All agencies will be responsible for implementation
2.information security is built into all public sector ICT systems from design through to implementation and disposal	Accepted	Agencies will work towards a minimum set of control measures taken from the accredited ISO standard	December 2013	On Track Draft minimum control set will be considered by the ICT Board in the third quarter 2012	All agencies will be responsible for implementation once the minimum control set is agreed.
3.all ICT products, services and assets adopted by agencies include common standards for information security, and in time a common and secure infrastructure is used across the public sector	Accepted	The ICT Strategy will enforce common standards for information security through compliance with or working towards a suitable ISO standard	December 2013	On Track The Information Security Working Group will recommend a minimum set of controls for adoption by the whole sector	All agencies
4.the processes by which Departments understand and manage their information risks are standardised	Accepted	NSW Treasury TPP 09-05 Internal Audit and Risk Management Policy supports greater standardisation of information security risk management practices		Completed	All agencies

Recommendation	Accepted or Rejected	Actions to be Taken	Due Date	Status and Comment	Responsibility
5.there is one central mechanism for establishing information assurance priorities, sharing risk information across agencies, and sharing best practice	Accepted	An information sharing network for the sector will be established as part of the implementation plan	Ongoing from third quarter 2012	The Information Security Working Group is reviewing the proposed approach	DFS facilitated, responsibility for participation will rest with all agencies
6.existing lines of accountability through Chief Executive Officers are used to improve information handling, with them signing off on the adequacy of security systems and information security to be included in their performance agreements	Accepted	Chief Executive Officers will sign a statement of attestation in their agency annual reports	From financial year 2013/2014	On Track	All agencies
7.mandatory training is provided to those with access to sensitive personal information or involved in managing it	Accepted with qualification	Agencies to ensure Code of Conduct addresses this issue	Ongoing	On Track	DFS will oversee implementation of the revised information security guidelines
8.action is taken to make clear that any failure to apply protective measures is a serious matter which could lead to dismissal	Rejected	The call for dismissal to be an option may be disproportionate to the conduct and difficult to implement from an evidentiary perspective			

Recommendation	Accepted or Rejected	Actions to be Taken	Due Date	Status and Comment	Responsibility
9.professional certification is required for staff or contractors working in roles with technical information security content	Accepted with qualification	Several qualifications and certifications exist to support this recommendation which would need to be considered by the ICT Leadership Group prior to possible acceptance	Jan 2013 through Dec 2014	To be investigated by the ICT Skills and Capability Development Working group	ICT Leadership Group decision
10.visibility of performance is increased, with agencies publishing material in their annual reports, and report to Parliament annually on information security across government	Accepted	See 6. above	From financial year 2013/2014	On Track	All agencies
11.there is truly independent monitoring of compliance, through audit and technical testing to a defined standard	Accepted for those agencies required to be certified	Proposal to require selected agencies/ Organisations to be certified under ISO 27001	Ongoing	On Track	Complying agencies such as shared service providers
12.agencies report breaches or near misses to an independent organisation responsible for capturing incidents, ensuring investigations are conducted, and lessons are learned .	Accepted with qualification	Proposal that breaches or near misses are reported to a co-ordinating body such that other agencies are informed at an appropriate time	Ongoing from third quarter 2012	The Information Security Working Group is reviewing the proposed approach	DFS with co-operation from agencies