Submission

No 11

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

Organisation: Audit Office of NSW

Name: Mr Peter Achterstraat

Position: Auditor General

Telephone: 9275 7100

Date Received:

Theme:

Summary

PA6489

audit office
OF NEW SOUTH WALES

Mr Jonathan O'Dea MP
Chair
Public Accounts Committee
Parliament House, Macquarie Street
SYDNEY NSW 2000

Attention Dr Abigail Groves

16 May 2012

Dear Mr O'Dea

Examination of the Auditor-General's Performance Audit Reports
Your letter of 10 May, Ref: LAC12/219

We have reviewed submissions provided by various agencies concerning the recommendations in the performance audit reports as mentioned below:

- Coal Mining Royalties – NSW Treasury
- NSW Public Sector Sick Leave
- Electronic Information Security

We are pleased to say that the agencies have accepted almost all recommendations. The submissions indicate that recommendations have either been implemented, on-going, or progress is being made.

Please find attached our comments on the progress reported by the agencies in relation to the recommendations in our original reports. We have not substantiated the submissions.

I am happy to provide any further assistance the Committee may need in completing its examination.

Yours sincerely

Peter Achterstraat
Auditor-General

Attachments

Performance Audit – Coal Mining Royalties – NSW Treasury – Implementation of recommendations

Recommendation	Accepted or rejected	Action to be taken	Due date	Status	Responsibility	Our comments
6. NSW Treasury, in consultation with DII and the Department of Premier and Cabinet, should undertake a detailed review of the merits of transferring the administration of royalties to the Office of State Revenue by June 2011 (page 16).	Accepted	NSW Treasury to form a working party along with representatives from Department of Industry and Investment, Office of State Revenue (OSR) and Department of Premier and Cabinet to review the merits of transferring administration of royalties to OSR.	Ongoing.	Working party formed in January 2011 and meetings were held in March and May 2011.	NSW Treasury remains responsible for the outcome of the working party.	Implementation is delayed. It would be helpful to know the outcomes of the meetings held so far and the expected timeframe for the working party to conclude its work and reach a decision.

Performance Audit – Sick Leave - Implementation of Recommendations

Recommendation	Accepted or rejected	Action to be taken	Due date	Status and comment	Responsibility	Our comments
1. We recommend that by September 2011, the Department of Premier and Cabinet help public sector agencies manage sick leave by sharing best practice examples of: a) agency strategies to reduce sick leave such as return to work interviews, welfare checks, and case managing staff with psychological issues (page 17) b) agency analysis of sick leave trends and patterns such as sick leave by weekday to help identify cases of excessive sick leave (page 18) c) monitoring sick leave with other human resource indicators including staff engagement to find out what motivates staff to go to work (page 18).	Accepted	An interagency working group to be convened to share best practice in relation to effective sick leave management	Sept 2011	Completed. The interagency meeting took place on 31 October 2011	Capability Group, Public Service Commission	DPC has advised this was achieved through the establishment of an inter-agency working group which met in October 2011. However there is not enough detail to determine how best practice examples will be shared with agencies.
2. We recommend that by February 2011, the Department of Premier and Cabinet provide agencies with the sick leave rates of all agencies in the NSW public sector so they can compare their performance (page 10).	Accepted	Provide each cluster head with a table comparing sick leave rates per FTE from 2008/9 and 2009/10 across the then 12 clusters. They were also to be provided with a breakdown of sick leave rates per FTE by agency within their cluster only.	February 2011	Completed. In February 2011, the information was provided to cluster heads.	Capability Group, Public Service Commission	DPC advises this information was provided to cluster heads in February 2011. It is not clear whether this practice will continue.
3. We recommend that by February 2011, the Department of Premier and Cabinet publish the average annual sick leave rate for the NSW public sector on its website to advise people of the public sector's performance (page 10).	Accepted	A revision is to be made to the NSW Public Sector Workforce 2010 Snapshot to include the average number of sick leave hours taken per FTE.	February 2011	Completed. In February 2011, a revision was made to the NSW Public Sector Workforce 2010 Snapshot to include at 4.9 the average number of sick leave hours taken per FTE: 1/56.88 hours compared to 56.78 hours the previous year". An increase of 0.18%.	Capability Group, Public Service Commission	This was completed in February 2011. It is not clear whether this practice will continue.

Performance Audit – Electronic Information Security - Implementation of Recommendations

Recommendation	Accepted or rejected	Action to be taken	Due date	Status and comment	Responsibility	Our comments
The Department of Premier and Cabinet should, on behalf of the NSW Government, publish a new Information and Communication Technology Strategy and establish new electronic information security governance arrangements by June 2011, and ensure that:						
1. minimum 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	Whilst taking longer than we had envisaged at the time of the report's release, the current timelines are reasonable and based on DPC's submission progress appears satisfactory.
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 2012	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 se tis agreed.	Based on DPC's submission, progress appears satisfactory.
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	Based on DPC's submission, progress appears satisfactory.
4. the processes by which agencies 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	Based on DPC's submission, the matter is finalised.
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.	Based on DPC's submission, progress appears satisfactory.
6. existing lines of accountability through Directors General and 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.	Based on DPC's submission, progress appears satisfactory.
7. mandatory training is provided to those with	Accepted	Agencies to ensure Code of	Ongoing	On track	DFS will oversee	Based on DPC's submission,

Recommendation	Accepted or rejected	Action to be taken	Due date	Status and comment	Responsibility	Our comments
access to sensitive personal information or involved in managing it	with qualification	Conduct addresses this issue.			implementation of the revised information security guidelines.	progress appears satisfactory.
8. action is taken to make clear that any failure to apply protective measures is a serious matter which could lead to disciplinary action	Rejected	Agencies to ensure Code of Conduct addresses this issue The call for dismissal to be an option maybe disproportionate to the conduct and difficult to implement from an evidentiary perspective.				The intent of this recommendation was that staff should be aware of the serious nature of a failure to adequately protect information. DPC's position, however, is acknowledged.
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	Based on DPC's submission, progress appears satisfactory.
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	Based on DPC's submission, progress appears satisfactory.
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	Based on DPC's submission, progress appears satisfactory.
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	Based on DPC's submission, progress appears satisfactory.