2012

Legislative Assembly for the Australian Capital Territory

Government submission to the Standing Committee on Public Accounts concerning the Auditor-General's Report No 2 of 2012

Whole of Government Information and Communications Technology Security Management and Services

Authorised for Publication

14 September 2012

Circulated by the authority of
Treasurer
Andrew Barr MLA

Government submission to the Standing Committee on Public Accounts concerning the Auditor-General's Report No 2 of 2012: *Whole of Government Information and Communications Technology Security Management and Services*

INTRODUCTION

The Auditor-General has reviewed the effectiveness of administrative structures and processes for whole-of-government ICT policies and procedures. Investigations by the Auditor General included addressing whether process, policies and procedures were well defined, managed and communicated. In doing this relevant information security and protective security issues were also considered.

Conclusions reached by the Auditor-General include that the protection of the ACT Government network is robust, and that our security regime has successfully defended against a large volume of attacks and unauthorised attempts to access the network over time. The audit noted some shortcomings provided some recommendations to strengthen the security environment.

The Auditor General's Report No. 2/2012 : *Whole of government Information and Communications Technology Security Management and Services* includes three recommendations. Those recommendations, and a Government position on those recommendations, are outlined below.

GOVERNMENT POSITION ON RECOMMENDATIONS / FINDINGS

Recommendation 1

Shared Services Division and Justice and Community Safety Directorates should improve whole-of-government security management practices by:

a) clarifying and documenting the roles and responsibilities of an ACT Government IT Security Advisor, the ACT Security in Government Committee and directorate Agency Security Advisors and their supporting communication processes. Directorates and agencies should be given information on these roles and responsibilities and communication processes once clarified (high priority); and

b) formalising the relationship between Security and Emergency Management Branch, and Shared Services ICT Security Section.

Government Position

Agreed.

The review of the *Protective Security Policy and Guidelines* has already commenced:

- Part 1 – to be completed by the end of October 2012 and will include reflecting machinery of government changes, clarification of roles, incorporation of relevant Australian and international information and ICT security standards, and noting that the ACT Government is considering moving to adopt the Commonwealth's mandatory framework for protective security.
- Part 2 – to be completed by 30 June 2013 and will define new mandatory framework for protective security, define compliance requirements under the new framework, and define the compliance monitoring and reporting system for ACT Government agencies.

Work is also underway to formalise the relationship between Security and Emergency Management Branch (SEMB) within Justice and Community Safety Directorate, and Treasury's Shared Services ICT (SSICT) branch.

Recommendation 2

The Justice and Community Safety Directorate through its leadership of the ACT Security in Government Committee should improve whole-of-government security management practices by:

a) establishing a process for surveying and reporting on compliance by directorates with approved information security policy, procedures and guidance material and using the results to inform review of these documents as required;

b) completing the review of the *Protective Security Policy and Guidelines* and in so doing:
- continue working to clarify which of the Commonwealth's 33 mandatory requirements for protective security, including information security, will be mandatory for ACT directorates and agencies;
- include references to international standards on information and ICT security (high priority);

c) addressing in its risk plan that not keeping information security policy and procedure current will restrict agencies ability to meet their information security obligations;

d) encouraging all directorates to include in their risk plans the risk of not being compliant with information security obligations and guidance; and

e) completing the current review of the operations of the ACT Security in Government Committee in relation to information security management.

Government Position

Agreed.

The review of the *Protective Security Policy and Guidelines* has already commenced (see response to Recommendation 1).

ACTSIGC has already reviewed its terms of reference and these were agreed by the Security and Emergency Management Senior Officials Group on 23 May 2012.

JACSD is updating its risk management plan and will add the risk of not keeping information security policy and procedures current. JACSD will encourage all Directorates to include in their risk plans the risk of not being compliant with information security obligations and guidance.

Recommendation 3

Shared Services Division should improve whole-of-government security management practices by:

a) advising directorates and agencies acquiring information services from private suppliers on potential security issues that may compromise the ACT Government's information security standards;

b) sponsoring the development of a mandatory requirement that:

- in general all directorates' and agencies' websites are hosted on the ACT Government network or by an ACT Government endorsed supplier; or
- where web applications are deployed on external hosts they should meet acceptable security, governance and change management standards; and
- web based applications that are not meeting acceptable security, governance and change management standards must be remediated or removed (high priority);

c) referencing international information and ICT security standards in key information security documents;

d) developing whole-of-government policies and procedures for managing ICT security in relation to new technologies, particularly for portable platforms (high priority);

e) fostering a mandatory requirement that directorates and agencies develop system security plans, and threat and risk assessments for:

- all new ICT systems; and
- legacy ICT systems using a risk analysis (high priority).

f) directing on-site teams to promote information and ICT security as part of their routine activities; and

g) planning for an ACT Government electronic records management system and pursuing funding for its implementation (high priority).

Government Position

Agreed parts (a) to (f).

Noted part (g).

System security plans are actively being developed for those systems that do not currently have them, with work to be undertaken jointly by Directorate business system owners, and SSICT Security advisors.

Existing website development and management policies and standards are being redeveloped as part of the Single Public Face project and include references to working with SSICT to ensure hosting arrangements are appropriate. Work is underway to redevelop a number of websites which will provide Directorates with the opportunity to migrate into a centralised supported arrangement. Current hosting arrangements are under review to provide greater scalability for Directorates looking to migrate hosting arrangements. Work is continuing in relation to a security review of all externally hosted websites.

All major ICT Security policy documents are under review and will be updated with references to ISO 27000 series standards as appropriate. This work is on track for the 1 January 2013 target date.

With respect to recommendation (g), the Information Strategy Committee, as a sub-committee of the Strategic Board, will take into consideration as part of their ongoing workplan, the future needs of government for an electronic records management system. Funding for this system / upgrade will be an issue for consideration in future budgets in line with whole-of-government priorities.