INTERNAL AFFAIRS
Te Tari Taiwhenua

19 December 2012

46 Waring Taylor St, PO Box 805
Wellington 6140, New Zealand
Telephone +64 4 495 7200
Facsimile +64 4 495 7222
Website www.dia.govt.nz

Iain Rennie
Head of State Services
State Services Commission
Level 10, Reserve Bank Building
2 The Terrace
Wellington 6140

Dear Iain

Review of Publicly Accessible Systems

"Repeated information privacy and security failings have the potential to undermine public confidence in our core government agencies and erode the relationship between citizen and state".

Privacy Commissioner, Marie Shroff

Background

On 16 October 2012, you asked me, in my role as Government Chief Information Officer, to undertake an urgent review of publicly accessible systems operated by State services. This was in the wake of a privacy and information security breach through publicly accessible kiosks in the Ministry of Social Development's Work and Income centres.

Good security and privacy policies, processes, and standards appropriately and consistently applied across the State services protect the reputation of government and help maintain public trust and confidence. My recommendations are aimed at building this trust and confidence.

Introduction

This review has given us a clear indication of the need to increase the level of maturity of agency systems and put in place appropriate controls, governance and (independent) assurance to ensure privacy and security. While many of the in-scope systems/agencies are clearly less than mature, it does not mean there are no protections in place, but that we have fallen short of providing a level of protection that the public would reasonably expect to be in place. These findings are consistent with the findings of the Deloitte review of information system security within the Ministry of Social Development.

Protection begins with having appropriately qualified staff who are able to identify security or privacy risks and routinely act to reduce or eliminate these risks. What this review shows is that in many cases across the State sector, there is an over reliance on our IT staff to manage privacy and security.

It is not enough to rely on staff, even excellent staff, alone. On top of this we need to treat information as an asset with its value and vulnerabilities recognised through proper management and stewardship. Security and privacy must also be an integral part of every business process, rather than separate disciplines. We need to design systems from the start to ensure that protection is in place, updated, and regularly tested. And finally, we need a robust documentation trail, which gives assurance to senior managers.

Privacy and security must be demonstrated through documented policies, processes, risk and assurance assessments, review and testing, and governance so the public can have confidence in government systems they use, or in which their information is stored.

Furthermore, as we work to increase online access to government services, more work will be required in this area. Our protection of secure and private information must not only keep pace, but get ahead of the service improvements we are making.

My full recommendations are attached at Appendix 1.

Below I outline the process I have used in undertaking my review. I also provide an overview of my findings and explain the actions taken to address high risk issues my review has identified. Finally, I explain the structure of my recommendations and highlight linkages to wider strategic management information work.

Review process

The purpose of the review is to provide Ministers with assurance on the security of publicly accessible systems, and to provide chief executives with advice on security improvements which can be made in the deployment and operation of such systems.

I released the terms of reference for the review on 19 October 2012. Subsequently I commissioned KPMG to carry out an assessment process based on the terms of reference. A copy of the KPMG assessment is attached.

The approach consisted of a review of documentation provided by agencies on security and privacy risk identification processes, and on governance structures such as roles, policies, standards and procedures in place to manage security and privacy issues.

After initial responses were received from agencies, I sought chief executive verification of each agency response.

Overview of review findings

Although there is evidence that good security and privacy practices exist within some agencies, the review has identified:

- a number (13) of high priority issues within the 215 in-scope systems;

- the security and privacy processes within many agencies lack maturity, and have an over reliance on the good technical skills and capabilities of staff and suppliers; and

- room for improvement in the support provided to agencies to aid compliance, through the provision of clear and coherent guidance and advice.

High priority issues identified and addressed

In total, 13 agencies were originally identified where unresolved vulnerabilities exist with publicly accessible systems. These vulnerabilities were identified because these particular agencies have more mature processes in place, in contrast to the majority of other agencies surveyed.

Of these 13 agencies, I am satisfied that 11 have taken appropriate action to fully address the risk. I have spoken directly to the Chief Executives of the remaining two agencies. These Chief Executives are aware of the issues, and have made clear decisions to accept the residual risk or to resolve the issue within a short timeframe.

The terms of reference for this review did not include explicitly testing for further similar vulnerabilities in agencies with less mature processes. Such vulnerabilities may, or may not, exist. My recommendations address this issue.

Structure of my recommendations

It is important that the principle of agency chief executive responsibility for security and privacy is reinforced. Consequently, I have structured my recommendations to cover immediate and short-term actions, which I recommend that agency chief executives should be directed to undertake to enhance current security and privacy practices within the State services.

Acknowledging the need for better support mechanisms, guidance and materials to aid agency compliance, I have also made recommendations designed to oversee and lift the quality of support available to agencies, over the longer term. This work will need to be linked with work already underway and led by the Government Statistician on the establishment of a privacy community of practice.

Wider strategic information management considerations

I believe it is important that any work arising out of this review be linked to work underway in the State Services Commission and the Department of Internal Affairs to review strategic information management policies and frameworks. This work includes consideration of an integrated strategic information management approach beyond the ICT-related aspects which are the subject of this review.

Communications

Before the recommendations are made public, I suggest that we jointly brief agency chief executives to explain the findings and to reinforce the need for immediate action on their part to address issues identified in the review.

Conclusion

Citizens need to have confidence that the private information they supply to government will be appropriately protected. Citizens also want to be able to interact with government in the most convenient way, which often involves the use of technology.

I believe my recommendations strike the appropriate balance of requiring immediate action from agency chief executives to improve security and privacy practices within their agencies, while developing more effective support mechanisms and materials to increase maturity over the longer term.

I am happy to discuss these recommendations with you directly and to support you in briefing Ministers as required.

Yours sincerely

Colin MacDonald
Government Chief Information Officer

Appendix 1

RECOMMENDATIONS

I recommend that agency chief executives are directed to:

1. **Immediately strengthen their information security and privacy general controls by:**
   - ensuring there is appropriate management and governance in place to monitor security and privacy practices;
   - implementing robust information security and privacy risk management practices, that are integrated with the agency's enterprise risk management framework;
   - requesting that audit committees and/or the internal audit programme consider information security and privacy as a priority part of their work programme; and
   - ensuring that there are appropriate levels of assurance over the agency's control environment.

2. **Immediately strengthen their information system controls by ensuring:**
   - any new system has a security risk assessment and privacy impact assessment undertaken, proportional to its inherent risk and the wider risk to the sector (relating to public confidence);
   - controls are designed to manage the risks;
   - there is executive oversight of risk identification and treatment; and
   - that the risks are re-assessed and controls assured on a regular ongoing basis.

3. **Within 3-6 months report to the Government Chief information Officer on:**
   - actions taken to improve the general IT controls environment;
   - a high-level view of the agency's ongoing programme to improve security and privacy systems and practices, or to review the effectiveness of security and privacy systems and practices where appropriate; and
   - confirmation that a full risk assessment of security and privacy is being undertaken as part of any new system design or modification.

I also recommend that you as Head of State Services:

4. **Establish an information privacy and security governance group chaired by the GCIO to oversee a security and privacy improvement work programme.**
   - This group to include: the State Services Commission; the Government Communications Security Bureau; the Office of the Privacy Commission; Statistics NZ; the Ministry of Business Innovation and Employment: the Department of the Prime Minister and Cabinet; and any other agencies as the Chair deems appropriate.

This governance group should be in place for a 2 year period, overseeing a work programme, which should include:

- developing a maturity model to ensure that mature security and privacy policies, processes, governance and standards are consistently applied across the State services;
- reviewing and revising existing information security and privacy guidance and, where appropriate, issuing clear, coherent and proportionate guidance on good information security and privacy practices; and
- developing solutions to support agency compliance, such as: training, education and information resources; consideration of cross-government contracts for IT security and privacy advisory and assurance services; and establishing a compliance and problem identification report-back mechanism and process from agencies.

5. **Direct me, as the GCIO, to report annually to you (for a two year period) on progress to improve information security and privacy across the State services.**