Office of the Minister of State Services

Chair
Cabinet Committee on State Sector Reform and Expenditure Control

REPORT OF THE GOVERNMENT CHIEF INFORMATION OFFICER ON THE REVIEW OF PUBLICLY ACCESSIBLE INFORMATION SYSTEMS

Proposal

1 This paper informs Cabinet of the findings and recommendations of the Review of Publicly Accessible Computer Systems recently undertaken by the Government Chief Information Officer on behalf of the State Services Commissioner, and the Commissioner's proposed response.

Executive summary

2 Following the recent security breach involving Ministry of Social Development Work and Income 'kiosks', the State Services Commissioner (the Commissioner) asked the Chief Executive of the Department of Internal Affairs, in his capacity as Government Chief Information Officer (GCIO), to undertake an urgent review of publicly accessible information systems operated by Government Departments and Crown Entities. The review report is attached at Appendix 1.

3 The urgency accorded to the review reflects the importance of maintaining public confidence in government systems. Without the public's confidence, work to increase online access to government services, (most notably through Results 9 and 10 of the Better Public Services work programme) and to make appropriate use of information across government, may be impacted.

4 The review finds that although there is evidence that good security and privacy practices exist within some agencies:

4.1 Within the 215 in-scope systems, 13 issues were identified as potentially high priority vulnerabilities that did not appear to have been addressed at the time of the initial review. Subsequently further documentation was provided to confirm action had been already taken to address one of these vulnerabilities prior to the review. Of the remaining 12, 11 of the vulnerabilities have been addressed by the agency responsible. One is under action now, and is expected to be addressed by the agency by 11 February.

4.2 The security and privacy processes within many agencies are under developed, and have an over reliance on the good technical skills and capabilities of staff and suppliers; and

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

5 In summary, the GCIO recommends to the Commissioner that:

5.1 Where required, agencies be directed to take steps to strengthen security and privacy governance, risk management, assurance and other controls

5.2 A programme of work is required to improve security and privacy practices across government, to be led by the GCIO with other key agencies, and including reviewing and revising security and privacy guidance and developing solutions to support agency compliance, taking account of current initiatives to improve security.

6 The review's recommendations strike an appropriate balance between requiring immediate action from agency chief executives to improve security and privacy practices within their agencies, and developing more effective support mechanisms and materials to increase performance in this area over the longer term. The Commissioner concurs with the recommendations of the GCIO and intends to work with the GCIO and State sector agencies to rapidly implement them.

7 To ensure that tangible progress and improvements in security performance can be demonstrated over the next 12 months and then on an ongoing basis, the Commissioner proposes expanding on aspects of some of the GCIO's recommendations.

8 Cabinet is asked to invite responsible Ministers to communicate directly to agency Chief Executives and Crown Entity Chairs its expectation that agencies will take the steps required to strengthen their security and privacy controls. Cabinet is also invited to note other related information security and privacy improvement work underway across the system.

Background

9 On 14 October 2012, freelance journalist Keith Ng alerted on his blog that he was able to access sensitive personal information from two 'kiosks' located in Work and Income offices in Wellington. The Ministry of Social Development took immediate steps to close access to the kiosks and launched a two phase independent review aimed at firstly determining what happened, and secondly, assessing the broader appropriateness and effectiveness of the Ministry's information security management settings. Reports on both phases of that review are now in the public domain. The Ministry is currently implementing a comprehensive response to the issues identified by the independent review.

10 On 16 October 2012 the Commissioner asked the Chief Executive of the Department of Internal Affairs, in his capacity as GCIO, to undertake an urgent review of publicly accessible information systems.

11 Terms of Reference for the review were released on 19 October 2012 and KPMG was appointed to assist the GCIO in responding to the terms of reference. An advisory group comprising the GCIO as chair, and members from the Department of the Prime Minister and Cabinet (DPMC), the Government Communications Security Bureau (GCSB) and the State Services Commission (SSC), was convened to support and advise the GCIO on the findings and resulting recommendations of the review. A representative of the Office of the Privacy Commissioner (OPC) also attended in an observer capacity.

12 The purpose of the review was to:

12.1 Provide Ministers with assurance on the security of publicly accessible systems

12.2 Provide Chief Executives with advice on security improvements which can be made in the deployment and operation of such systems.

13 Due to the urgency the review was accorded, the terms of reference confined matters within scope to publicly accessible systems including:

13.1 Kiosks or similar devices that provide public access that are connected to a Government network

13.2 Web services that provide a service delivery interface; and

13.3 Wireless networks providing access to the public.

14 However, the recommendations arising from the review extend beyond improving publicly accessible systems, and have been designed to assist State service Chief Executives to lift overall agency capability in respect to security and privacy.

15 The GCIO presented the KPMG assessment together with his recommendations to the State Services Commissioner on 19 December 2012. The Commissioner appreciates the work undertaken by the GCIO and agencies within tight timeframes.

Methodology of the KPMG Assessment

16 The assessment undertaken by KPMG looked at security documentation from 70 Departments and Crown Entities relating to 215 systems comprising 'kiosks', websites used for personal information transactions, and wireless networks. It also looked at the controls, oversight and assurance arrangements within which systems were deployed.

17 The security applied over the publicly accessible systems, and the wider security practices used by agencies, was assessed by performing a desk-based review of documentation provided by the in-scope agencies. KPMG also reviewed the independent reports commissioned by MSD in response to the kiosk security breach. Unlike the independent review commissioned by MSD in response to the kiosk security breach, the KPMG assessment did not involve undertaking security tests on specific systems.

18 While the KPMG assessment did not include security testing, phase three of the Cybersecurity Plan for Government Information and Assets (due for completion on 8 February 2013) requires 35 Chief Executives of core Government Departments to identify high value/risk information assets, conduct a risk-assessment, and create and implement a plan to reduce risk to an acceptable level.

19 The KPMG assessment found that:

19.1 Within the 215 in-scope systems, 13 issues were identified as potentially high priority vulnerabilities that did not appear to have been addressed at the time of the initial review. Subsequently further documentation was provided to confirm action had been already taken to address one of these vulnerabilities prior to the review. Of the remaining 12, 11 of the vulnerabilities have been addressed by the agency responsible. One is under action now, and is expected to be addressed by the agency by 11 February.

19.2 The security and privacy processes within many agencies are under developed, and have an over reliance on the good technical skills and capabilities of staff and suppliers; and

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

20 The KPMG assessment also found that while there are some examples of good practice, there are patterns of practice that do not meet expectations. With regard to the publicly accessible systems for which documentation was reviewed, KPMG found:

20.1 There is limited evidence that robust security risk management processes are in place

20.2 There is limited evidence that security and privacy controls are being explicitly designed into publicly accessible systems

20.3 There is limited evidence that organisations are seeking assurance over their publicly accessible systems or security management processes

20.4 Most agencies using third party systems are doing so without assessing the security of those systems; and

20.5 Many kiosk systems are more vulnerable to security breaches than other publicly accessible systems.

21 However, sometimes controls exist in undocumented form. Given the review relied on agency provided documentation, KPMG was not able to assess whether un-documented controls exist within agencies.

22 With respect to security governance more generally within agencies, the KPMG assessment found that:

22.1 Most agencies have security policies in place, but many are not supported by standards and procedures, and most lack formal robust security risk management processes

22.2 Accountability for security varies across agencies, but is often not clearly defined; and

22.3 There is limited evidence that agencies are seeking assurance over their compliance with the Security in the Government Sector (SIGS) framework or the New Zealand Information Security Manual (NZISM).

23 On the basis of this assessment, and taking into account the findings of MSD's recent Independent Review of Information Security, KPMG provided advice on a non-exhaustive set of actions and considerations to lift agency capability with respect to security and privacy where this was needed. This advice is listed at pages 14-19 of the KPMG Assessment (attached at Appendix 1).

Recommendations of the GCIO to the Commissioner

24 The GCIO's recommendations, which are based on the KPMG assessment and the GCIO's work across the system, reinforce the principle of agency chief executive responsibility for security and privacy. The recommendations are split into two categories. The first covers immediate and short-term actions that are necessary to enhance current security and privacy controls within the State services. The second category of recommendations is designed to lift the quality of support mechanisms, guidance and materials available to agencies dealing with privacy and security issues.

Need to strengthen controls

25 The GCIO recommends to the State Services Commissioner that agency Chief Executives be directed to immediately strengthen their information security and privacy general controls by:

25.1 Ensuring there is appropriate management and governance in place to monitor security and privacy practices

25.2 Implementing robust information security and privacy risk management practices, that are integrated with the agency's enterprise risk management framework

25.3 Requesting that audit committees and/or the internal audit programme consider information security and privacy as a priority part of their work programme; and

25.4 Ensuring that there are appropriate levels of assurance over the agency's control environment.

26 He also recommends that agency Chief Executives be directed to immediately strengthen their information systems controls by ensuring:

26.1 Any new system has a security risk assessment and a privacy impact assessment undertaken, proportional to its inherent risk and the wider risk to the sector (relating to public confidence)

26.2 Controls are designed to manage the risks

26.3 There is executive oversight of risk identification and treatment; and

26.4 That the risks are re-assessed and controls assured on a regular ongoing basis.

27 The GCIO recommends that agencies report to him within 3 to 6 months 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 with confirmation that a full risk assessment of security and privacy is being undertaken as part of any new system design or modification.

Information security and privacy improvement work-programme

28 The GCIO also recommends that the Commissioner establish a governance group chaired by the GCIO to oversee an information security and privacy improvement work programme. This group should include SSC, GCSB, the Office of the Privacy Commissioner, Statistics New Zealand, MBIE, DPMC, and any other agencies the State Services Commissioner and Chair deem appropriate;

29 The GCIO considers that the governance group should be in place for a 2 year period, overseeing a work programme which should include:

29.1 Developing a model to ensure that mature information security and privacy policies, processes, governance and standards are consistently applied across the State services

29.2 Reviewing and revising existing information security and privacy guidance and, where appropriate, issuing clear, coherent and proportionate guidance on good information security privacy and practices; and

29.3 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.

30 The GCIO recommends that the Commissioner directs him to report annually (for a two year period) on progress to improve information security and privacy across the State services.

State Services Commissioner's proposed response to GCIO recommendations

31 The Commissioner accepts all of the GCIO's recommendations and is pleased that implementation activities are underway, and critical issues have already been addressed. Given the importance of addressing the problems identified by this Review, the Commissioner particularly welcomes the fact that implementation of these recommendations will provide Ministers with a broad level of assurance. It is crucial that tangible progress, and improvements in security performance can be

demonstrated over the next 12 months and then on an ongoing basis. To this end, the Commissioner intends to expand on aspects of the recommendations as follows:

31.1 Require the governance group to investigate the use of standardised security and privacy reporting across the State sector (GCIO recommendation 4). Over time, this will help to improve the consistency and comparability of security and privacy performance information. Standardised reporting will be designed to incorporate agencies' existing security and privacy reporting requirements. Additional reporting requirements may include looking at what information should be included in Annual Reports to Parliament.

31.2 Clarify that Chief Executives, as part of their reporting to GCIO on progress, will specify how they intend to demonstrate improvements, where necessary, to their security and privacy systems and practices (GCIO recommendation 3). It is intended that this reporting is tailored to agencies' functions and size as well as the maturity of its security and privacy systems.

31.3 Lead work, in close consultation with the governance group, on system-level mapping of governance and operational roles in the information security and privacy area. A number of agencies, including DIA, DPMC, GCSB, NZSIS, and SSC have mandated roles within the security and privacy area. This work will look at how those roles intersect, how respective work programmes can be aligned, and how to best support the improvements the review has established are required.

32 In addition, SSC and the Office of the Privacy Commissioner are currently discussing how Chief Executives' responsibility for privacy and security matters can be further reinforced within the overall framework for setting Chief Executive performance expectations. The Office of the Privacy Commissioner will have observer status in the proposed new governance group.

Implementation of the GCIO's recommendations

33 Implementation of the review recommendations has commenced. In December 2012, GCIO wrote to agency Chief Executives asking them to ensure that they have sought appropriate advice from their responsible managers and assured themselves that all necessary steps have been taken to immediately strengthen their information security and privacy general controls (as outlined in paragraphs 25 -27).

34 Furthermore, in October 2012, the GCIO and the Commissioner wrote to Departments and Crown Entities asking that Chief Executives take immediate steps to assure themselves that their publicly accessible systems are secure in compliance with the policies, standards and guidelines contained in the Security in Government Sector (SIGS) and NZ Information Security Manual (NZISM).

35 The Commissioner recently briefed departmental Chief Executives in writing on the findings and recommendations of the review. The 13 agencies that were identified as having high priority information security issues were also briefed. Crown Entities will be briefed following Cabinet's consideration of the review, but before it is publicly released. Departmental Chief Executives will also be invited to a meeting to discuss the improvements to privacy and security controls that need to occur, and how their agency will be supported throughout that process.

36 To ensure Chief Executives can access appropriate support, the State Services Commissioner and GCIO, in consultation with the information privacy and security governance group, and other agencies as required, will establish a panel of privacy and security expertise that can be accessed by agencies requiring assistance with

implementing the GCIO's recommendations. The panel would consist of private sector suppliers, who would be required to apply all relevant government security and privacy standards to their work.

37 The Commissioner intends to make the review, its findings and recommendations, and his response public via a press release following Cabinet's consideration of the review. I seek Cabinet's authorisation to release a copy of this paper at the same time. The Commissioner will work with my office on this release.

38 Responsible Ministers are invited to communicate directly to agency Chief Executives and Crown Entity Chairs Cabinet's expectation that agencies will move quickly to implement the findings of the review. A template letter will be provided to Ministers.

Related work

39 Implementation of the GCIO's recommendations is part of a wider set of issues relating to managing information as an asset. Other work underway includes:

39.1 The State Services Commission is leading a group of senior officials looking at broader information management issues at a system level. Work underway includes developing a framework for dealing with strategic information policy issues (led by DIA) and sharing best practice in information privacy management (led by Statistics New Zealand). The Privacy and Information Security Governance Group established by the review will now lead and coordinate this work.

39.2 The National Cyber Policy Office (NCPO) in DPMC has assumed responsibility for implementation of New Zealand's Cyber Security Strategy. The Strategy identifies protection of Government Systems and Information as a priority, with two key deliverables aimed at improving security in this area. First, in July 2011 Cabinet approved a Cybersecurity Plan for Government Information and Assets. Secondly, in September 2011 the National Cyber Security Centre was established within GCSB to build on existing cyber security and information assurance capabilities to provide enhanced protection of government systems and information against advanced and persistent threats.

39.3 The Law Commission's review of the Privacy Act 1993. The Law Commission's recommendations to increase the enforcement powers of the Privacy Commissioner are currently being examined by the Ministry of Justice.

39.4 The Information Sharing Bill currently before Parliament will increase the ability of government agencies to share information relating to common clients where there are good reasons.

39.5 The Vulnerable Kids Information System which, once implemented, will be a key element of the Government's Vulnerable Children strategy. The system will allow Government agencies and frontline professionals to access information specific to the children they are working with, when they need it. Community based agencies contracted to deliver services to vulnerable children and their families will also have appropriate access. Before the system is implemented in late 2014 a code of conduct will be in place on safe sharing of information about vulnerable children by the end of 2013. Security of information will be paramount.

39.6 The Advisory Expert Group on Information Security (AEGIS), which will provide advice, and report to, the Vulnerable Children's Board, as the body responsible for implementing the Children's Action Plan. The aim of establishing AEGIS was to ensure that there was independent oversight and public certainty about the information sharing arrangements for the Children's Teams, the Vulnerable Kids Information System and the Predictive Risk Modelling Tool.

39.7 The review of SIGS, led by NZSIS.

39.8 The work of the ICT Strategy Taskforce.

40 These work streams will be aligned with the activities of the information security and privacy governance group, to ensure that security and privacy work under way across the system is appropriately coordinated.

Consultation

41 The Department of Internal Affairs, Government Chief Information Officer, Government Communications Security Bureau, and Statistics New Zealand were consulted on this paper and were also members of the Advisory Group for the GCIO Review of Publicly Accessible Systems. The Ministry of Business, Innovation, and Employment, the Ministry of Social Development and the Ministry of Justice were also consulted on this paper. The Department of Prime Minister and Cabinet and the Privacy Commissioner were informed of this paper.

Financial implications

42 None.

Human rights implications

43 None.

Legislative implications

44 None.

Regulatory impact analysis

45 None.

Gender implications

46 None.

Disability perspective

47 None.

Publicity

48 The Commissioner intends to make the report, its findings and recommendations, and his response public via a press release following consideration of this report by Cabinet and once agency Chief Executives have been briefed. I seek Cabinet's agreement to release a copy of this paper at the same time. Requests for comment should be directed to the Commissioner in the first instance.

Recommendations

49 It is recommended that the Committee:

1 **Note** the attached report of the Government Chief Information Officer's (GCIO) *Review of Publicly Accessible Systems* (the Review), commissioned by the State Services Commissioner;

2 **Note** that the State Services Commissioner accepts all of the recommendations contained in the Review;

3 **Note** that although there is evidence that good security and privacy practices exist within some agencies, the Review identified:

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

3.2 The security and privacy processes within many agencies are under developed, and have an over reliance on the good technical skills and capabilities of staff and suppliers; and

3.3 Room for improvement in the support provided to agencies to aid compliance, through the provision of clear and coherent guidance and advice;

High Priorities Identified and Addressed

4 **Note** that potentially high priority vulnerabilities relating to 13 agencies within the 215 in-scope systems were identified, and that of the 13 potential vulnerabilities:

4.1 Subsequent documentation was provided to confirm that action had been taken to address one of the vulnerabilities prior to the review;

4.2 11 have been addressed by the agency responsible;

4.3 One is under action now and is expected by the agency to be resolved by 11 February;

Need to strengthen controls

5 **Agree** that agencies should immediately strengthen their information security and privacy general controls by:

5.1 Ensuring there is appropriate management and governance in place to monitor security and privacy practices;

5.2 Implementing robust information security and privacy risk management practices, that are integrated with the agency's enterprise risk management framework;

5.3 Requesting that audit committees and/or the internal audit programme consider information security and privacy as a priority part of their work programme; and

5.4 Ensuring that there are appropriate levels of assurance over the agency's control environment;

6 **Agree** that agencies should immediately strengthen their information systems controls by ensuring:

6.1 Any new system has a security risk assessment and a privacy impact assessment undertaken, proportional to its inherent risk and the wider risk to the sector (relating to public confidence);

6.2 Controls are designed to manage the risks;

6.3 There is executive oversight of risk identification and treatment; and

6.4 That the risks are re-assessed and controls assured on a regular ongoing basis;

7 **Note** that the GCIO has written to all in-scope agency Chief Executives asking them to ensure that they have sought appropriate advice from their responsible managers and assured themselves that all immediate necessary steps have been taken, including those steps in recommendations 5 and 6 above;

8 **Agree** that agencies report within 3 to 6 months to the GCIO on:

8.1 Actions taken to improve the general IT controls environment

8.2 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;

8.3 Confirmation that a full risk assessment of security and privacy is being undertaken as part of any new system design or modification;

9 **Note** that the State Services Commissioner intends to require agencies to specify how they will demonstrate increased security of their systems, where action is required;

10 **Invite** the State Services Commissioner and responsible Ministers to communicate directly to agency Chief Executives and Crown Entity Chairs Cabinet's expectation that agencies will take the steps outlined in recommendations 5, 6 and 8 above;

Information security and privacy improvement work-programme

11 **Note** that the State Services Commissioner will establish an information privacy and security governance group for a two year period to oversee an information security and privacy improvement work programme, to be chaired by the GCIO and to include the State Services Commission, the Government Communications Security Bureau, Statistics New Zealand, the Ministry for Business Innovation and Employment, the Department of the Prime Minister and Cabinet, and any other agencies the State Services Commissioner and the Chair deem appropriate;

12 **Note** that the Office of the Privacy Commissioner will be invited to participate as an observer in the privacy and security governance group in recommendation 11;

13 **Note** that the work programme overseen by the information security and privacy governance group will include:

13.1 Developing a model to ensure that well developed information security and privacy policies, processes, governance and standards are consistently applied across the State Services;

13.2 Reviewing and revising existing information security and privacy guidance and, where appropriate, issuing clear, coherent and proportionate guidance on good information security privacy and practices;

13.3 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;

14 **Note** that the State Services Commissioner intends to require the security and privacy governance group to investigate the use of standardised security and privacy reporting across the State sector in order to improve the consistency and comparability of security and privacy performance information over time;

15 **Note** that the development of standardised security and privacy reporting will be designed to incorporate agencies' existing security and privacy reporting requirements;

16 **Note** that the State Services Commissioner intends to require Chief Executives, as part of their reporting to GCIO on progress, to specify how they intend to demonstrate the increased security of their systems and that this reporting will be tailored to agencies' functions and size as well as the maturity of their security privacy systems;

17 **Note** that the State Services Commissioner, in close consultation with the governance group, will lead work on mapping governance and operational roles in the information security and privacy area;

18 **Note** that the State Services Commissioner and GCIO in consultation with the security and privacy governance group, and other agencies as required, will establish a panel of privacy and security expertise that can be accessed by agencies requiring assistance with implementing the GCIO's recommendations;

19 **Note** that the State Services Commissioner will request that the GCIO will report annually to him (for a two year period) on progress to improve information security and privacy across the State Services;

20 **Note** that the State Services Commissioner intends to publish the findings and recommendations of the Review following Cabinet's consideration of this paper, and once agency Chief Executives have been briefed;

21 **Authorise** the Minister of State Services to release a copy of this Cabinet paper at the time the Review is published.

Hon Jonathan Coleman
Minister of State Services

____/____/____