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 proposed response to the review.

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. Subsequent documentation was provided to confirm that action had been taken to address one of the vulnerabilities prior to the review. Of the remaining 12, all have been addressed by the agency responsible;

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 The review's recommendations address these serious, systemic issues through a combination of:

5.1 Urgent remedial actions to lift the security of State sector IT systems and practices;

5.2 Mechanisms to drive and support agency compliance with the review recommendations; and

5.3 New GCIO-mandated security and privacy reporting requirements, and an escalation process for poorly performing or non-compliant agencies.

6 Cabinet is invited to direct Chief Executives and Board Chairs that within one month agencies should make a strategic choice to either:

6.1 Continue to operate publicly facing systems and uplift their IT capability to meet on-going security and privacy challenges; or where this is not possible

6.2 Seek alternative arrangements such as utilising capability in other agencies, to ensure appropriate security and privacy levels are achieved and maintained.

7 Implementation of these recommendations will ultimately be the responsibility of individual agency Chief Executives. However, GCIO with support from Central Agencies will be responsible for monitoring implementation activities and escalating matters to SSC where necessary.

8 The Commissioner concurs with the recommendations of the GCIO and intends to work with the GCIO and State sector agencies to rapidly implement them. Among other measures, the Commissioner plans to reinforce Chief Executives' responsibility for security and privacy issues through the Chief Executive performance expectation setting process. The Commissioner will also begin to consult with the GCIO and the Office of the Privacy Commissioner about agencies' security and privacy performance as part of the Chief Executive performance review process.

9 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.

Background

10 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.

11 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.

12 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.

13 The purpose of the review was to:

13.1 Provide Ministers with advice and assurance on the security of publicly accessible systems; and

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

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

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

14.2 Web services that provide a service delivery interface; and

14.3 Wireless networks providing access to the public.

15 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.

16 The GCIO presented the KPMG assessment together with his recommendations to the Commissioner in December 2012. After further consideration and discussion, the Commissioner has agreed with the GCIO a more detailed set of proposed actions to ensure that the required improvements to agency information security and privacy controls are implemented as a matter of priority. The Commissioner appreciates the work undertaken on the review by the GCIO and participating agencies.

Methodology of the KPMG Assessment

17 The assessment undertaken by KPMG looked at security documentation from 70 Departments and Crown Entities relating to 215 systems. It also looked at the controls, oversight and assurance arrangements within which systems were deployed.

18 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.

19 While the KPMG assessment did not include security testing, the Cybersecurity Plan for Government Information and Assets (CSP) requires 35 Chief Executives of core Public service and non-Public service departments to improve the security of IT within their agencies. The CSP was approved by Cabinet in May 2011 and is currently being implemented by GCSB, DIA, and the National Cyber Policy Office. A progress report on the implementation of risk-based processes for addressing the cyber security of agencies systems is due to Cabinet shortly.

20 The KPMG assessment found that:

20.1 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. Subsequent documentation was provided to confirm that action had been taken to address one of the vulnerabilities prior to the review. Of the remaining 12, all have been addressed by the agency responsible;

20.2 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

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

21 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:

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

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

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

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

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

22 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.

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

23.1 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;

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

23.3 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).

24 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).

Agreed recommendations from the GCIO to the Commissioner

25 The GCIO's recommendations, which are based on the KPMG assessment and the GCIO's work across the system, balance the principle of agency Chief Executive responsibility for security and privacy matters with high-level oversight of, and support for implementation of the recommendations.

26 The recommendations are split into two categories:

26.1 The first covers immediate improvements to lift the security of State sector IT systems and practices;

26.2 The second relates to mechanisms to drive and support agency compliance with the review recommendations; and

27 If agreed by Cabinet, the GCIO will coordinate, and where necessary enforce implementation of the recommendations. GCIO's role will be supported by Central Agencies. Coordination and enforcement of the recommendations fits within the GCIO's existing Cabinet mandate to provide leadership on ICT matters within government.

Immediate improvements to the security of IT systems and practices

28 The GCIO's recommendations prioritise remedial actions to lift the security of IT systems and practices. The recommendations have three components:

28.1 Implementing measures to lift the maturity of security practices and strengthen controls;

28.2 Testing currently deployed in-scope systems; and

28.3 Ensuring information system controls are in place for new systems.

29 The recommendations sequence actions according to their urgency. Together, these actions represent critical first steps to restore public confidence in information systems across the State sector.

30 The GCIO will provide advice to agencies on the actions proposed in these recommendations.

Implement measures to lift the maturity of security practices and strengthen controls

31 The GCIO recommends that agency Chief Executives be directed to take immediate action to strengthen their information security and privacy general controls by:

31.1 Ensuring that IT security is treated as integral to the conduct of agency business rather than solely as an IT issue;

31.2 Assigning executive team level leadership and accountability for information security and privacy, and ensuring this is strongly linked with broader security and information management roles within the organisation;

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

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

31.5 Ensuring agencies review arrangements with suppliers and assure themselves that systems currently in place comply with security standards (NZISM, SIGs and others as relevant); and

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

32 Cabinet is invited to direct Chief Executives and Board Chairs that within one month agencies should make a strategic choice to either:

32.1 Continue to operate publically facing systems and uplift their IT capability to meet on-going security and privacy challenges; or, where this is not possible

32.2 Seek alternative arrangements such as utilising capability in other agencies, to ensure appropriate security and privacy levels are achieved and maintained.

Testing currently deployed in-scope systems

33 The GCIO Review recommends technical security assessments of all in-scope publicly accessible systems (where it has not already been carried out). The GCIO has recommended technical security assessments are carried out according to the following timeline:

33.1 within 1 month, those agencies not in scope of the CSP will complete a detailed risk assessment of their publicly accessible systems (with coordination from the GCIO), and provide the results of the risk assessment to the GCIO;

33.2 within 4 months, agencies will complete a security assessment over any high risk systems that have not been assessed in the past 18 months, and

33.3 within 12 months, agencies will complete a security assessment over all other publicly facing systems that have not been assessed in the past 18 months;

34 The GCIO further recommends that agencies should immediately, upon identification, report to the GCIO on any vulnerabilities identified through the technical security assessment of their publicly accessible systems, along with a plan to address those vulnerabilities.

Ensure information system controls are in place for new systems

35 The GCIO has recommended that agencies immediately strengthen their information systems controls by ensuring:

35.1 Any new system, including those purchased “off-the-shelf”, 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);

35.2 A framework and process is in place to certify and accredit systems before they are placed into production; and

35.3 That the risks are re-assessed and controls assured on a regular ongoing basis (not less than every 18 months).

36 The GCIO has also recommended that within 4 months agencies will provide it with:

36.1 Confirmation that it has undertaken all of the actions set out in paragraphs 31 - 34 that are required to be completed within 4 months and that plans are in place for those actions for which a longer time frame is required;

36.2 A statement of capability, setting out how it has implemented the above actions and how the agency is discharging its accountabilities; and

36.3 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.

Mechanisms to drive and support agency compliance

37 These recommendations are intended ensure actions arising from the review have senior oversight, are well prioritised and adhered to.

Reporting requirements and escalation process

38 To ensure agency compliance with the suite of recommendations outlined above, and to ensure the GCIO maintains an overview of risk across the system, the GCIO has recommended that:

38.1 agencies with identified high priority vulnerabilities that are unresolved or accepted, must report that risk to the GCIO;

38.2 agencies are directed to consult the GCIO on plans to address any high-priority system vulnerabilities identified; and

38.3 the GCIO may escalate agency compliance issues to the State Service Commissioner for discussion with the agency chief executive and, where necessary, the responsible Minister and the Minister for State Services.

39 These recommendations place permanent, ongoing reporting obligations on agencies.

40 In addition, the Commissioner has asked the GCIO to report to him on initial security and privacy improvements within 6 months and on the ongoing improvement programme annually to him (for a two year period) on progress to improve information security and privacy across the State sector. The Commissioner and the GCIO will jointly report to the Minister of State Services on the initial security and privacy improvement measures within 6 months, and on the ongoing improvement work programme annually for a two year period.

Accessing market capability

41 The urgent action to improve IT security across agencies (described in paragraphs 31-36) will put pressure on scarce high-quality security resources within the marketplace, and that this will need to be carefully managed to ensure quality and cost effectiveness.

42 To manage demand and ensure value for money, the GCIO and the Commissioner, in consultation with the security and privacy governance group (proposed in paragraph 44), and other agencies as required, will establish a panel of privacy and security expertise (the panel) that can be accessed by agencies requiring assistance with implementing the GCIO's recommendations. Cabinet is invited to direct agencies to use the panel.

43 The panel will report on its assessments of information security processes and system security within agencies to the GCIO and agency chief executives.

Enhancing system level security governance

44 The GCIO recommends the State Services Commissioner establishes an information privacy and security governance group (the governance group) to oversee a tightly focussed information security and privacy improvement work programme across the system. The group will operate for a two year period to

ensure that the required improvements are not just implemented but can be measured and sustained.

45 It is proposed that the governance group will be chaired by the GCIO and will include SSC, GCSB, Statistics New Zealand, MBIE, DPMC, and any other agencies the Commissioner and the Chair deem appropriate. The Office of the Privacy Commissioner will be invited to participate as an observer.

46 The governance group's work programme will take account and leverage the work of the CSP, and other relevant government security standards (SIGS, ISM and PSM), and will include:

46.1 by July 2013, developing a model to ensure that integrated information security and privacy policies, processes, governance and standards are consistently applied across the State Services;

46.2 by September 2013, review and revise existing information security and privacy guidance and, where appropriate, issuing clear, coherent and proportionate guidance on good information security privacy and practices;

46.3 by September 2013, investigate the use of standardised security and privacy reporting across the State sector. Standardised reporting will help to improve the consistency and comparability of security and privacy performance information and will be designed to incorporate agencies' existing security and privacy reporting requirements. This may include looking at what information should be included in Annual Reports to Parliament; and

46.4 by September 2013, develop solutions to support agency compliance and build security and privacy capability within agencies, such as training, education and information resources, and establishing a compliance and problem identification report-back mechanism and process from agencies.

47 In addition, the Commissioner will 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.

Chief Executive performance expectations

48 The Commissioner will reinforce Chief Executives' responsibility for security and privacy issues within their agency through Chief Executive performance expectations. The Commissioner will also consult with the GCIO and the Office of the Privacy Commissioner about agencies' security and privacy performance as part of the Chief Executive performance review process.

Ministerial endorsement of recommendations

49 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 (where they have not already done so). A template letter will be provided to Ministers.

Related work

50 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:

50.1 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.

50.2 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.

50.3 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.

50.4 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.

50.5 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.

50.6 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.

50.7 The review of SIGS, led by NZSIS.

50.8 The work of the ICT Strategy Taskforce.

51 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

52 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

53 None.

Human rights implications

54 None.

Legislative implications

55 None.

Regulatory impact analysis

56 None.

Gender implications

57 None.

Disability perspective

58 None.

Communications on the GCIO Review

59 To ensure swift implementation of the GCIO's recommendations, communication with State sector Chief Executives on the findings of the review commenced in October 2012, when 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).

60 In December 2012, the 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.

61 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.

62 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. The Commissioner will work with my office on this release. Requests for comment should be directed to the Commissioner in the first instance.

Recommendations

63 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;

4 **Note** that in May 2011, Cabinet approved the Cyber Security Plan for Government Information and Assets (CSP), which is currently being implemented by the Government Communications Security Bureau, the Department of Internal Affairs, and the National Cyber Policy Office, to improve the cyber security of IT systems in 35 core public service and non-public service departments

5 **Note that** a progress report on the implementation of risk-based processes for addressing the cyber security of agencies systems is due to Cabinet shortly.

6 **Note** that implementation of the GCIO's recommendations will ultimately be the responsibility of individual agency Chief Executives but that the GCIO, with support from Central Agencies, will be responsible for monitoring implementation activities and escalating matters to SSC where necessary;

High Priorities Identified and Addressed

7 **Note** that of the 13 potentially high priority vulnerabilities that did not appear to have been addressed at the time of the initial review:

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

7.2 Of the remaining 12, all have been addressed by the agency responsible;

Immediate improvements to the security of IT systems

Implement measures to lift the maturity of security practices and strengthen controls

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

8.1 Ensuring that security is treated as integral to the conduct of agency business rather than solely as an IT issue;

8.2 Assigning executive team level leadership and accountability for information security and privacy and ensure this is strongly linked with broader security and information management roles within the organisation;

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

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

8.5 Ensuring agencies review arrangements with suppliers and assure themselves that systems currently in place comply with security standards (NZISM, SIGs and others as relevant);

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

9 **Direct** Chief Executives and Board Chairs that within one month agencies should make a strategic choice to either:

9.1 Continue to operate publically facing systems and uplift their IT capability to meet on-going security and privacy challenges,

or

9.2 where this is not possible, seek alternative arrangements such as utilising capability in other agencies, to ensure appropriate security and privacy levels are achieved and maintained;

Testing currently deployed in-scope systems

10 **Agree** that the GCIO will coordinate technical security testing of all in-scope publicly accessible systems (where it has not already been carried out) according to the following timeframes:

10.1 within 1 month, those agencies not in scope of the CSP will complete a detailed risk assessment of their publicly accessible systems (with coordination from the GCIO), and provide the results of the risk assessment to the GCIO;

10.2 within 4 months, agencies will complete a security assessment over any high risk systems that have not been assessed in the past 18 months, and

10.3 within 12 months, agencies will complete a security assessment over all other publicly facing systems that have not been assessed in the past 18 months;

11 **Agree** that agencies should immediately, upon identification, report any vulnerabilities identified through the technical security assessment of their publicly accessible systems proposed in Recommendation 10, along with a plan to address those vulnerabilities, to the GCIO;

Ensure information system controls are in place for new systems

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

12.1 Any new system, including those purchased "off-the-shelf", 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);

12.2 A framework and process is in place to certify and accredit systems before they are placed into production;

12.3 That the risks are re-assessed and controls assured on a regular ongoing basis (not less than every 18 months);

13 **Agree** that within 4 months agencies will provide to the GCIO:

13.1 Confirmation that it has undertaken all of the actions set out in recommendations 9 - 11 that are required to be completed within 4 months and that plans are in place for those actions for which a longer time frame is required;

13.2 A statement of capability, setting out how it has implemented actions in recommendations 9-11 and how the agency is discharging its accountabilities;

13.3 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;

14 **Note** that the GCIO will provide advice to agencies on the actions proposed in recommendations 9 to 13;

Mechanisms to drive and support agency compliance

General reporting requirements and escalation process

15 **Agree** that agencies, that have identified high priority vulnerabilities that are unresolved or accepted, must report that risk to the GCIO;

16 **Direct** agencies to consult the GCIO on plans to address any high-priority system vulnerabilities identified;

17 **Agree** that the GCIO may escalate agency compliance issues to the State Service Commissioner for discussion with the agency chief executive and, where necessary, the responsible Minister and the Minister for State Services;

18 **Note** that recommendations 15-17 place permanent, ongoing reporting obligations on agencies;

19 **Note** that the State Services Commissioner will request that the GCIO will report on initial security and privacy improvements within 6 months and on the ongoing improvement programme annually to him (for a two year period) on progress to improve information security and privacy across the State Services;

20 **Invite** the State Services Commissioner, in consultation with the GCIO, to report to the Minister of State Services on the initial security and privacy improvement measures within 6 months, and on the ongoing improvement work programme annually for a two year period;

Accessing market capability

21 **Note** urgent action to improve IT security across agencies will put pressure on scarce high-quality security resources within the marketplace, and that this will need to be carefully managed to ensure quality and cost effectiveness;

22 **Agree** that the State Services Commissioner and GCIO, in consultation with the security and privacy governance group proposed in recommendation 25, and other agencies as required, will establish a panel of privacy and security expertise (the panel) that can be accessed by agencies requiring assistance with implementing the GCIO's recommendations;

23 **Direct** agencies to use the panel;

24 **Agree** that the panel will report on its assessments of information security processes and system security within agencies to the GCIO and agency chief executives;

Enhancing system level security governance

25 **Note** that the State Services Commissioner will establish an information privacy and security governance group (the governance group) to oversee a tightly focussed information security and privacy improvement work programme across the system;

26 **Note** that the group will operate for a two year period to ensure that the required improvements are not just implemented but can be measured and sustained;

27 **Note** the governance group will be chaired by the GCIO and will 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;

28 **Note** that the Office of the Privacy Commissioner will be invited to participate as an observer in the governance group;

29 **Note** that the work programme overseen by the governance group will take account and leverage the work of the CSP and other relevant government security standards (SIGS, ISM and PSM), and will include:

29.1 by July 2013, developing a model to ensure that well developed and integrated information security and privacy policies, processes, governance and standards are consistently applied across the State Services;

29.2 by September 2013, 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;

29.3 by September 2013, investigate the use of standardised security and privacy reporting across the State sector. This may include looking at what information should be included in Annual Reports to Parliament.

29.4 by September 2013, developing solutions to support agency compliance and build security and privacy capability within agencies, such as training, education and information resources, and establishing a compliance and problem identification report-back mechanism and process from agencies;

30 **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;

Chief Executive performance expectations

31 **Note** that the State Services Commissioner will reinforce Chief Executives' responsibility for security and privacy issues within their agency through Chief Executive performance expectations;

32 **Note** that the State Services Commissioner will begin to consult with the GCIO and the Office of the Privacy Commissioner about agencies' security and privacy performance as part of the Chief Executive performance review process;

Ministerial support for GCIO Review recommendations

33 **Invite** 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 9-24 above;

Communications on the GCIO review

34 **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 to secure their publicly accessible systems;

35 **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;

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

Hon Tony Ryall

Acting Minister of State Services

____/____/____