Cabinet Committee on State Sector Reform and Expenditure Control

SEC Min (13) 2/6

Copy No:

Minute of Decision

Report of the Government Chief Information Officer on the Review of Publicly Accessible Information Systems

Portfolio: State Services

On 26 February 2013, the Cabinet Committee on State Sector Reform and Expenditure Control (SEC):

Background

1 **noted** that on12 February 2013, SEC:

1.1 noted the report entitled *Government Chief Information Officer's Review of Publicly Accessible Systems* (the Review), commissioned by the State Services Commissioner (the Commissioner) and the contents of the submission on the Review;

1.2 directed the Commissioner, in consultation with the Government Chief Information Officer (GCIO) and relevant departments, to report to SEC with a revised submission with additional proposals to:

1.2.1 address agency capacity and capability in information security and privacy controls;

1.2.2 ensure that the required improvements to agency information security and privacy controls are implemented as a matter of priority;

[SEC Min (13) 1/3]

Government Chief Information Officer's Review

2 **noted** the Review attached to the submission under SEC (13) 5;

3 **noted** that the Commissioner accepts all of the recommendations contained in the Review;

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

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

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;

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

5 **noted** that:

5.1 in May 2011, the Cabinet Committee on Domestic and External Security approved the *Cyber Security Plan for Government Information and Assets* (CSP) [DES Min (11) 1/3];

5.2 the CSP 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;

6 **noted** that a progress report on the implementation of risk-based processes for addressing the cyber security of agencies systems is due to be considered by Cabinet shortly;

7 **noted** 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 the State Services Commission (SSC) where necessary;

High Priorities Identified and Addressed

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

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

8.2 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

9 **agreed** that agencies immediately strengthen their information security and privacy general controls by:

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

9.2 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;

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

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

9.5 ensuring agencies review arrangements with suppliers and assure themselves that systems currently in place comply with security standards (Security in the Government Sector (SIGS), New Zealand Information Security Manual (NZISM) and others as relevant);

9.6 ensuring that there are appropriate levels of assurance over the agency's control environment;

10 **directed** chief executives and invite Crown Entity chairs that within one month agencies should make a strategic choice to:

Either:

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

Or:

10.2 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

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

11.1 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;

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

11.3 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;

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

Ensure information system controls are in place for new systems

13 **agreed** that agencies should immediately strengthen their information systems controls by ensuring:

13.1 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);

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

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

14 **agreed** that within 4 months agencies will provide to the GCIO:

14.1 confirmation that it has undertaken all of the actions set out in paragraphs 10-12 above 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;

14.2 a statement of capability, setting out how it has implemented actions in paragraphs 10-12 above and how the agency is discharging its accountabilities;

14.3 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;

15 **noted** that the GCIO will provide advice to agencies on the actions in paragraphs 10-14 above;

Mechanisms to drive and support agency compliance

General reporting requirements and escalation process

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

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

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

19 **noted** that the decisions in paragraphs 16-18 above place permanent, ongoing reporting obligations on agencies;

20 **noted** that the Commissioner will request that the GCIO 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;

21 **invited** the 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

22 **noted** that 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;

23 **agreed** that the Commissioner and GCIO, in consultation with the security and privacy governance group in paragraph 26 below, and other agencies as required, establish a panel of privacy and security expertise (the panel) that can be accessed by agencies requiring assistance with implementing the GCIO's recommendations;

24 **directed** agencies to use the panel;

25 **agreed** 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

26 **noted** that the 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;

27 **noted** 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;

28 **noted** the governance group will be chaired by the GCIO and will include SSC, 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 Commissioner and the Chair deem appropriate;

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

30 **noted** 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, NZISM and the Protective Security Manual), and will include:

30.1 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;

30.2 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;

30.3 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);

30.4 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;

31 **noted** that the 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

32 **noted** that the Commissioner will reinforce chief executives' responsibility for security and privacy issues within their agency through chief executive performance expectations;

33 **noted** that the 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

34 **invited** responsible Ministers to communicate directly to agency chief executives and Crown Entity chairs Cabinet's expectation that agencies will take the steps outlined in paragraphs 10-25 above;

Communications on the GCIO review

35 **noted** 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;

36 **noted** that the Commissioner intends to publish the findings and recommendations of the Review following Cabinet's consideration, and once agency chief executives have been briefed;

37 **authorised** the Minister of State Services to release a copy of the submission under SEC (13) 5 at the time the Review is published.

Committee Secretary Reference: SEC (13) 5