Office of the Minister of State Services

Chair

Cabinet Economic Growth and Infrastructure Committee

UPDATE ON IMPLEMENTATION ACTIONS ARISING FROM THE GOVERNMENT CHIEF INFORMATION OFFICER'S REVIEW OF PUBLICLY ACCESSIBLE SYSTEMS

Proposal

1 This paper updates Cabinet on early implementation actions arising from the Government Chief Information Officer's Review of Publicly Accessible Systems.

Executive summary

2 Implementation actions following on from the review of publicly accessible systems by the Government Chief Information Officer (GCIO) have advanced according to the Cabinet-agreed work programme. These actions are central to restoring and then maintaining the New Zealand public's confidence in the State Sector's ability to securely handle personal information.

3 All agencies have complied with the Cabinet-agreed work programme and are taking their response to the review seriously.

4 The results of the one-month actions have provided agencies and the GCIO with a better understanding of how to prioritise further assurance work (for example, penetration testing) across the system. The GCIO's new security services supplier panel will ensure that agencies' access to scarce private-sector security capability is managed in the most cost- effective manner.

5 Further testing on internet-based publicly accessible systems belonging to the 12 agencies with identified (resolved) security vulnerabilities has revealed a number of new vulnerabilities. The GCIO has worked with agencies to ensure mitigation strategies are in place to address the vulnerabilities and that risk mitigation strategies are agreed at a senior leadership level within the 12 agencies. The new vulnerabilities have now either been resolved, or managed to the satisfaction of the relevant business owner.

6 The identification of new vulnerabilities is a common outcome of the assurance process. The nature of threats to IT systems is constantly evolving, meaning new vulnerabilities will always emerge. One of the key outcomes of further work by the GCIO and the Information Security and Privacy Governance Group (Governance Group) is to ensure agencies and the system are set up to continuously review and refresh security management within a wider risk framework.

7 A number of system-level improvement actions have been running alongside individual agency responses to the Cabinet-agreed work programme. These include work to set up a single, coordinated point of assurance on government ICT (through the GCIO), an update to Chief Executive performance expectations to reinforce their responsibility for security and privacy issues within their agency and the establishment of the Cabinet-mandated Governance Group.

8 I propose to release the review and associated Cabinet papers in late May. The State Services Commission and GCIO are working with my office, the office of the Minister of Internal Affairs, and agencies within the scope of the review to manage this release.

Background

9 On 16 October 2012, the State Services Commissioner (the Commissioner) asked the GCIO to undertake an urgent review of publicly accessible systems.

10 The purpose of the review was to:

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

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

11 The review looked at security documentation from 70 Departments and Crown Entities relating to 215 publicly accessible systems.

12 The review found that:

12.1 Within the 215 in-scope systems, 12 agencies were identified as having potentially high priority vulnerabilities, all of which had been addressed by the agency responsible by January 2013;

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

12.3 There was room for improvement in the support provided to agencies to aid compliance with information security and privacy standards, through the provision of clear and coherent guidance and advice.

13 The GCIO presented his report and recommendations to the Commissioner in December 2012. He also wrote to in-scope agency Chief Executives asking them to ensure that they had sought appropriate advice from their responsible managers and had assured themselves that all necessary steps have been taken to immediately strengthen their information security and privacy general controls.

14 In February 2013, following further consideration and discussion, the Commissioner and the GCIO agreed a more detailed work programme to ensure that the required improvements to agency information security and privacy controls were implemented as a matter of priority.

15 In March 2013 Cabinet agreed to the GCIO's recommended work programme [CAB Min (13) 6/2D refers]. On 28 March 2013, the 70 agencies within the scope of the review were each instructed by their responsible Minister to commence implementation of the work programme.

16 In March 2013, the Minister of Internal Affairs and I deferred the public release of the report to allow for further testing to be carried out on internet-based publicly accessible systems belonging to the 12 agencies which had originally been identified as having high priority security vulnerabilities (now addressed). This decision was taken following advice from Government Communications Security Bureau (GCSB) and the National Cyber Policy Office (NCPO) that identifying the 12 agencies would create a clear and identifiable target for principal threat actors' (for example, hackers) activities. GCSB and NCPO advised that further assurance and mitigation activities should be carried out before the 12 agencies were publicly identified.

Implementation actions taken since March 2013

17 Implementation actions to date fall into three categories:

17.1 Actions agencies were required to take within one month of the Cabinet-agreed work programme commencing;

17.2 Further testing on internet-based publicly accessible systems belonging to the 12 agencies; and

17.3 System-level actions, led by the Commissioner and the GCIO.

18 Progress in each category is discussed in paragraphs 19 – 33.

One month actions (due by 26 April 2013)

19 Public Service Chief Executives and Crown Entity Board Chairs within the scope of the review were instructed to make a strategic decision to either:

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

20 Agencies were required to report their decisions to the GCIO. The GCIO provided advice and assistance to agencies making this assessment.

21 Agencies were also required to complete a detailed risk assessment of their publicly accessible systems and to provide the results to the GCIO.[1]

22 One month actions were designed to help agencies prioritise further assurance work (for example, penetration testing).

Results of one month actions

23 All in-scope agencies have submitted their one month action responses to the GCIO.

24 At this stage, all agencies have elected to continue to operate their publicly accessible information systems and uplift their capability to meet on-going security and privacy challenges. Following agencies' completion of four-month actions (see paragraph 34), the GCIO will have sufficient information about agencies' improvement programmes to make informed judgements on where capability may need to be further supported. At this point, and as information security and privacy standards are lifted, agencies will need to reflect further on whether they have the capability to meet on-going security and privacy challenges. The GCIO will work with agencies to support them to do this.

25 In future, increased use of common capabilities (such as Infrastructure as a Service and the Common Web Platform) and proposed clustering of IT capability will support the required uplift in security and privacy practices by requiring greater interagency collaboration.

26 Some agencies with more advanced assurance programmes have moved beyond risk assessment to security testing. The GCIO is also providing guidance to agencies to ensure that access to scarce private-sector information security capability is prioritised and managed in a cost-effective manner. In the short term, agencies are being offered access to private sector information security capability

[1] Agencies within the scope of the Cyber Security Plan were asked to provide their Cyber Security Plan assessment.

through the Department of Internal Affairs' existing panel of security services suppliers.

27 The GCIO is establishing a new all-of-Government security services supplier panel which, once in place, will be mandatory for agencies to use. The new supplier panel will provide an expanded range of services to agencies including:

- Source code and application review
- Network and application testing (including penetration testing)
- Risk assessment and assurance (including privacy impact)
- Policy and security consulting and advisory
- Security architecture and design; and
- Investigation and forensics.

28 From information provided to the GCIO and from discussions with agencies, it appears a number of Chief Executives and Chairs are still delegating oversight of security assessment work to their IT security function rather than approaching this work with a wider risk management view. The GCIO, supported by the Commissioner and the Governance Group, will continue to encourage greater involvement and oversight by Chief Executives or Board Chairs in these processes.

29 There is also a need to integrate security and privacy within a wider and ongoing information management risk framework. The GCIO and Governance Group will support this through the provision of further education and guidance.

Further assurance activities relating to the 12 agencies' publicly accessible systems

30 Further testing on the 12 agencies' internet-based publicly accessible systems is now complete[2]. As expected, a number of additional vulnerabilities have been identified.

31 The GCIO has worked with agencies to ensure mitigation strategies are in place to address each vulnerability and that risk mitigation strategies are agreed at a senior leadership level within the 12 agencies. The new vulnerabilities have now either been resolved, or managed to the satisfaction of the relevant business owner. The new vulnerabilities could have only been exploited through a targeted, deliberate and malicious unlawful attack.

32 The identification of new vulnerabilities is a common outcome of the assurance process. The nature of threats to IT systems is constantly evolving, meaning new vulnerabilities will always emerge. One of the key outcomes of further work by the GCIO and the Governance Group is to ensure agencies and the system are set up to continuously review and refresh security and privacy management processes.

System-level actions

33 A number of system-level actions have been running alongside individual agencies' responses to the Cabinet-agreed work programme:

33.1 The Cabinet-mandated Information Security and Privacy Governance Group [CAB Min (13) 6/2D refers] has been established and has met twice. The Governance Group is responsible for ensuring:

[2] Internet-based publicly accessible systems have been the focus of assurance activities because they were the most vulnerable to attack.

- Recommendations arising from the review are not just implemented but can be measured and sustained; and
- Security and privacy work underway across the State sector is well co-ordinated.

33.2 The Commissioner has reinforced Public Service Chief Executives' responsibility for security and privacy issues within their agency through an update to Chief Executive performance expectations.

33.3 The Commissioner instructed all Public Service Chief Executives to provide him with assurance on actions they have taken to reduce the likelihood of the unintentional release of private information via email. The State Services Commissioner also recommended to other State Sector agencies (for example, Crown Entities) that they perform a similar assurance exercise and report to their Board on the findings. All Public Service Departments have responded with risk assessments or high level actions regarding their email systems. Most agencies are undertaking additional work in response to their assessments, including:

- Implementing the actions outlined in the recent GCIO email circular and the Privacy Action Plan
- Staff training and awareness; and
- The roll out of data loss prevention software.

The State Services Commission has linked agencies requiring assistance in this area with the GCIO.

33.4 The GCIO has released a circular containing advice to agencies on how to prevent the unintentional release of private information via email and has been working with agencies on practical solutions to prevent such unauthorised disclosure.

33.5 A Privacy Leadership Programme, led by Statistics New Zealand has developed a toolkit of privacy resources, which has been published on the Public Sector Intranet. The toolkit is already in active use by a number of agencies and feedback has been positive. The Privacy Leadership Programme has also invited proposals from selected contractors for developing a privacy assessment framework for the public sector. This is expected to be completed by September 2013.

33.6 The National Cyber Security Centre within GCSB has released a bulletin on proactive measures agencies should be undertaking to improve information security within their agencies, such as deploying patches.

33.7 Work to set up a single, coordinated point of assurance on Government ICT (through the GCIO) has progressed, as has work to clarify the role and mandate of the GCIO. This will be progressed as a companion paper to the Government ICT Strategy and Action Plan to go to Cabinet in June.

Next steps – four-month actions (due by end of July)

34 Agencies within the scope of the review are currently working on four-month actions. Agencies' four-month report back will be an important milestone because it will provide further detail on agencies' programmes of improvement. At this point agencies must provide the GCIO with:

- a statement of capability, setting out how they have implemented immediate, 1 and 4 month actions;

- a high-level view of their ongoing programme to improve security and privacy systems and practices, or to review their effectiveness where appropriate;
- confirmation that they have undertaken all of the prescribed immediate, one month and four month actions; and
- any vulnerabilities identified through security assessments, along with plans to address those vulnerabilities.

35 The Commissioner and GCIO will report to the Minister of State Services and Minister of Internal Affairs in September 2013 on the results of the four-month actions (as part of previously agreed reporting schedule [CAB Min (13) 6/2D refers]).

Publicity

36 In March 2013, Cabinet noted that the Commissioner intends to make the review, and its findings and recommendations public via a press release. Cabinet also authorised me to release the Cabinet paper on the review [CAB Min (13) 6/2D refers].

37 I seek Cabinet's agreement to release a copy of this paper and associated Cabinet Minutes at the same time other material on the review is publicly released.

38 Public release of material relating to the review is planned for late May. The State Services Commission is working with my office, the Minister of Internal Affairs' office and agencies within the scope of the review on this release.

39 Public comment will be led by the State Services Commissioner and GCIO with myself and the Minister of Internal Affairs providing comment from Ministers. Requests for comment on matters relating to the review should be directed to the Commissioner in the first instance.

40 The 12 named agencies may also be approached for comment. To manage this each of the 12 agencies will be requested to prepare and place on their website a statement setting out the steps they have taken since the review to address potential vulnerabilities and improve security. Requests for further comment on release day will be referred to the State Services Commission or lodged under the Official Information Act.

41 If media enquire further about an individual agency's systems over subsequent days this will need to be managed by the agency concerned. The State Services Commission will work closely with agencies if this occurs, keeping my office informed.

Consultation

42 The Government Chief Information Officer, the Department of Internal Affairs, the Government Communication Security Bureau, the Ministry of Business, Innovation, and Employment, Statistics New Zealand, the Ministry of Social Development, the Inland Revenue Department, the Ministry of Justice, the New Zealand Security Intelligence Service, and the Office of the Privacy Commissioner were consulted on this paper. The Department of the Prime Minister and Cabinet including the National Cyber Policy Office was informed of this paper.

Financial implications

43 Implementation actions arising from the review are being met through in-scope agencies' baselines.

Human rights implications

44 None.

Legislative implications

45 None.

Regulatory impact analysis

46 Not applicable.

Gender implications

47 None.

Disability perspective

48 Not applicable.

Recommendations

49 It is recommended that the Committee:

1 **Note** that implementation actions associated with the GCIO Review of Publicly Accessible Systems have progressed according to the Cabinet-mandated work programme;

2 **Note** the Minister of State Services' intention to publicly release the GCIO Review of Publicly Accessible Systems at the end of May 2013;

3 **Authorise** the Minister of State Services to release this Cabinet paper and associated Cabinet Minute at the same time the GCIO Review of Publicly Accessible Systems is released.

Hon Dr Jonathan Coleman
Minister of State Services

____/____/____

1. Security weak points identified in publicly accessible computer systems

These potential vulnerabilities were identified as part of the review of publicly accessible computer systems carried out by the GCIO in late 2012 and represents a 'snap shot' at that time.

These potential vulnerabilities have been addressed.

There is no evidence any of these potential vulnerabilities has led to a breach of privacy.

Agency	Description	Status
Careers New Zealand	Kiosks were connected to an internal network.	Resolved
Ministry for Culture and Heritage	Visitor kiosk and meeting room computer were connected to the internal network.	Resolved
Department of Corrections (MECF)	Prisoners at Mt Eden Corrections Facility were able to access a limited number of external websites through a prisoner kiosk.	Resolved
Ministry of Education	A system had a vulnerability to potential access by unauthorised users.	Resolved
EQC	A system had a vulnerability to potential access by unauthorised users.	Resolved
Commission for Financial Literacy and Retirement Income	A system had password strength and reset process vulnerabilities.	Resolved
Ministry of Justice	Maori Land Court kiosks were connected to an internal network.	Resolved
Maritime New Zealand	A system had password strength and reset process vulnerabilities.	Resolved
MidCentral DHB	A kiosk for patients to access the Internet was connected to an internal network.	Resolved
New Zealand Trade and Enterprise	Wireless network encryption on first level of authentication not best practice.	Resolved
Ministry of Social Development	A system had a vulnerability to potential access by unauthorised users.	Resolved
Tertiary Education Commission	A system had password strength and reset process vulnerabilities.	Resolved

2. State Sector agencies within the scope of the GCIO Review (excluding the 12 agencies with identified security vulnerabilities)

The following State Sector agencies had publicly accessible systems and were therefore within the scope of the GCIO Review of Publicly Accessible Systems.

ACC
Auckland DHB
Bay of Plenty DHB
Canterbury DHB
Capital and Coast DHB
CERA
Civil Aviation Authority of New Zealand
Clerk of the House of Representatives
Counties-Manukau DHB
Crown Law Office
Customs
Department of Conservation
Department of Internal Affairs
DPMC
Education Review Office
Electoral Commission
Environmental Protection Agency
GCSB
Hawkes Bay DHB
Housing New Zealand Corporation
Hutt Valley DHB
IRD
Lakes District DHB
LINZ
Ministry for Business, Innovation, and Employment
Ministry for Primary Industries
Ministry for the Environment
Ministry of Defence
Ministry of Foreign Affairs and Trade
Ministry of Health
Ministry of Pacific Island Affairs
Ministry of Transport
Ministry of Women's Affairs
Nelson-Marlborough DHB
New Zealand Antarctic Institute
New Zealand Blood Service
New Zealand Defence Force
New Zealand Fire Commission
New Zealand Lotteries Commission
New Zealand Qualifications Authority
New Zealand Transport Agency
Northland DHB
NZ Police
NZSIS
Parliamentary Counsel Office
Parliamentary Service
Public Trust
SFO
South Canterbury DHB
Southern DHB
SSC
Statistics New Zealand
Tairawhiti DHB
Taranaki DHB
Te Puni Kōkiri
Tertiary Education Commission
The Treasury
Waikato DHB
Wairarapa DHB
Waitemata DHB
West Coast DHB
Whanganui DHB

3. State Sector agencies that were outside the scope of the GCIO Review

The following State Sector agencies had no publicly accessible systems and were therefore outside of the scope of the GCIO Review of Publicly Accessible Systems.

Annuitas
Broadcasting Standards Authority
Commerce Commission
Creative New Zealand
Drug-free Sport
Education New Zealand
EECA
Electricity Authority
External Reporting Board
Families Commission
Financial Markets Authority
Health and Disability Commissioner
Health Promotion Agency
Health Quality and Safety Commission
Historic Places Trust
Human Rights Commission
Independent Police Conduct Authority
International Accreditation New Zealand
Law Commission
Maori Language Commission
New Zealand Artificial Limb Board
New Zealand Film Commission
New Zealand on Air
New Zealand Superannuation Fund
New Zealand Symphony Orchestra
Office of Film and Literature Classification
Office of the Children's Commissioner
Pharmac
Productivity Commission
Real Estate Agents Authority
Social Workers Registration Board
Sport New Zealand
Standards NZ
Takeovers Panel
Te Mangai Paho
Te Papa
Teachers Council
Tourism New Zealand
Walking Access Panel