Office of the Minister of State Services
Office of the Minister of Internal Affairs

Chair
Cabinet Committee on State Sector Reform and Expenditure Control

INITIAL IMPROVEMENTS TO INFORMATION PRIVACY AND SECURITY AND PLAN OF ACTION TO APRIL 2015

Proposal

1 This report provides a progress update on privacy and security improvements since the GCIO Review of Publicly Accessible Information Systems (GCIO Review) in November 2012; sets out an action plan to lift and sustain capability across the State sector; and, seeks agreement to publicly release a copy of this report after it has been considered by Ministers.

Executive summary

2 Following the GCIO Review, Cabinet directed the GCIO to undertake a range of actions to improve privacy and security capability across the State sector [Cab Min (13) 6/2D refers] and report back to us on progress after six months.

3 Lifting capability is critical to restoring and maintaining public trust and confidence in the way that government agencies manage citizens' private information. The success of Government objectives to increase online access to services and to make smarter use of information relies on the confidence of the public.

4 Good progress has been made in improving privacy and security capability over the last six months:

- Agencies have completed security assessments of all high risk publicly accessible information systems. As a result of this process, there is greater confidence in the security of those publicly accessible information systems.
- Additional vulnerabilities were identified through this process but none were of the same level as the previous round of testing. Remediation plans have been put in place. The identification of new vulnerabilities is an expected outcome of any security assessment process.
- Agencies are reporting an uplift in practice and understanding of privacy and security matters and have plans to further improve their capability by March 2014. The GCIO will continue to provide advice and support to agencies over the interim period to help them meet their capability targets.
- The expectations on agencies have been clearly set and risk assessment tools, guidance on security assessments, and indicators of best practice have been provided to support agencies in meeting these expectations.
- A security services panel has been implemented to assist agencies in accessing scarce capability. The panel will also help drive consistency, cost effectiveness and transparency.
- A privacy leadership toolkit has been published with guidance and examples of tools and practice for agencies to use. A privacy maturity assessment framework is currently being piloted with agencies.

5 While progress has been good, and to plan, considerable ongoing work is still required. A plan of action for the next 18 months is attached to this paper at **Appendix A**. This work programme, together with the GCIO's ongoing engagement with agencies, will ensure agencies continue to be supported and provided with guidance and tools while a streamlined framework to support sustained system-wide improvement is developed. The framework will set clear expectations for how information privacy and security should be governed and managed, support agencies in meeting these expectations, monitor progress and provide assurance that expectations are being met.

6 Improving and sustaining capability in information privacy and security will require Chief Executives and Board Chairs to drive behavioural change through their organisations. Ongoing senior level focus will be required once the framework is implemented to manage the ongoing risk to privacy and security of information and to embed improvements into organisations.

Background

7 Following the Ministry of Social Development (MSD) kiosk security breach in October 2012, the State Services Commissioner asked the GCIO to undertake an urgent review of publicly accessible information systems.

8 The purpose of the review was to provide Ministers with advice on the security of publicly accessible systems and provide Chief Executives with advice on security improvements that can be made in the operation of these systems. KPMG was engaged to provide assistance to the GCIO in assessing responses from agencies.

9 The KPMG assessment looked at security documentation from 70 departments and Crown Entities relating to 215 systems. The KPMG assessment, together with the GCIO recommendations, was presented to Cabinet in March 2013.

10 The review's findings identified that security and privacy processes within many agencies were under-developed and there was a need to build understanding of security and privacy within a wider risk management frame.

11 The review's recommendations sought to address these issues through urgent remedial actions to lift the security of State sector ICT systems and practices as well as mechanisms to drive and support agency compliance.

12 To oversee this work, an Information Privacy and Security Governance Group, chaired by the GCIO, was established for a two year term to April 2015. This group has been tasked by Cabinet to ensure a sharp and sustained focus on improving information privacy and security matters.

Initial improvements in privacy and security – what has changed over the last six months

Security assessments of publicly accessible information systems

13 Agencies in the review's scope were directed by Cabinet to undertake risk assessments of their publicly accessible information systems by April 2013 and to undertake security assessments of their high risk systems by the end of July.

14 All agencies have completed risk assessments of, and have confirmed they will continue to operate, their publicly accessible information systems. In doing so, these agencies have committed to undertake a programme of improvement to lift practice and capability in privacy and security.

15 All agencies have completed security assessments of their high risk publicly accessible information systems. Agencies are required to confirm to the GCIO that they have completed security assessments of their remaining medium and low risk systems by March 2014. From discussions with agencies it appears that many have already progressed this.

16 As expected, vulnerabilities were identified though the security assessment process. These vulnerabilities have either been remediated or remediation plans are in place, agreed at a senior level. No high priority vulnerabilities with an impact on privacy were reported through this process.

17 The nature of threats to ICT systems is constantly evolving. The identification of new vulnerabilities is an expected outcome of the security assessment process and mitigates the potential for, but does not entirely remove the risk of, further breaches.

18 Privacy and security breaches are often the result of human error and not always the result of ICT system vulnerabilities. For this reason, Chief Executives and Board Chairs need to continue to ensure their organisations are appropriately managing this risk on an ongoing basis.

Actions to improve practice and capability within agencies

19 Agencies were asked to complete a self assessment of their capability as at the end of July and their planned capability by March 2014, based on a capability maturity model. All agencies have provided these statements to the GCIO. The GCIO has also been engaging with agencies as part of its ongoing relationship function to further inform a view of capability in privacy and security across agencies.

20 The level of capability maturity needed will depend on the information holdings of an agency. Not every agency is expected to have the highest possible level of maturity. In addition, lifting maturity often relies on a behavioural and cultural change, which takes time to embed into an organisation. For these reasons, we consider that some agencies may be optimistic in their plans to lift maturity over the next 8 months.

21 At a summary level, agencies are reporting an uplift in practice and understanding since November 2012, with improvement across all indicators and further investment in improvements planned.

22 Areas that have significantly improved since November 2012 relate to security governance and accountability:

- 98% of agencies now have a Chief Information Security Officer and/or an IT Security Manager appointed compared to 50% in November 2012.
- 98% of agencies have reported that accountability for privacy and security is at the executive level compared to 21% in November 2012.
- All agencies plan to further improve their security governance by March 2014 by putting in place structures and processes that enable security and privacy to be considered in the context of the agency business.

23 Maturity in security risk management and accreditation and certification, as reported by agencies, has improved slightly.

- 84% of agencies now have a formal security policy in place compared with 73% in November 2012. All agencies plan to have a formal policy in place, supported by standards, by March 2014.
- 30% of agencies now have formal risk management processes in place compared to 27% in November 2012. This is not a significant improvement, however,

almost all agencies plan to have formal processes that are documented, and consistently followed, by March 2014.

- 40% of agencies now have a security accreditation and certification process in place compared to 13% in November 2012. The majority of these processes, however, have not been formally documented.

24 While positive, these movements are not as significant. This is to be expected over a six month period given the low levels of maturity indicated in the initial GCIO Review. It will take time and investment to significantly improve maturity in these areas.

25 The next report-back for agencies will be at the 12 month mark, in March 2014. At this point, agencies are required to confirm they have completed security assessments of all medium and low risk publicly accessible information systems, and will also be asked to report on progress against their improvement plans.

26 The GCIO will continue to support agencies over this period through the new security services panel and by facilitating the sharing of experience from agencies with higher levels of capability. Targeted assistance will be provided to agencies with a lower level of maturity. The GCIO ICT Assurance function will monitor ICT operational risk to target interventions where appropriate and provide advice to agencies and Ministers where necessary.

27 The information received from agencies on their current and planned level of capability provides a benchmark for future measurement of progress. When agencies report again in March 2014, the degree of progress made will determine the level of engagement or intervention needed from the GCIO in order to provide assurance to Ministers that privacy and security risks are being managed appropriately.

28 Ministers will receive a further report on progress, based on the results of the 12 month report back from agencies, by June 2014.

Accessing market capability

29 Capability and capacity in the security and privacy area is limited. To assist agencies in accessing the resources they need, an all of government common capability panel for security and related services has been established. The panel is intended to enable a lift in risk, security and privacy management performance through a common approach by all government agencies. This panel will provide agencies with expertise to support their ongoing improvement plans.

30 The panel is mandatory for public service and non-public service departments and is available to all State sector agencies.

31 The GCIO will receive information on all panel engagements to assist in targeting assurance interventions. Agencies will also receive support from the GCIO in accessing services from the panel to drive consistency and cost effectiveness.

32 This is an open panel, meaning suppliers that wish to join the Panel, or add additional service categories, after it has been established can do. Additional categories will be added to the panel over time. This will include broadening privacy related services.

Expectations, guidance and support

33 We have set clear expectations in relation to improving privacy and security practice, which have been supported by the GCIO. These expectations have been reinforced in communications from Ministers to all agencies and in performance expectations for Chief Executives.

34 Cabinet has tasked the Information Privacy and Security Governance Group with:

- reviewing and revising existing guidance and issuing clear guidance on good practice where appropriate;
- developing solutions to support agency compliance and build security and privacy capability within agencies; and
- establishing a problem identification report-back mechanism and process from agencies.

35 Progress on these tasks is set out in the sections below.

Information security

36 Significant work has been done to support improved information security practice. The GCIO has provided tools to assist agencies to undertake risk assessments of their publicly accessible information systems and guidance on security assessments to help agencies access the right services. To assist agencies in developing their statements of capability, a capability maturity model has been developed with indicators of good practice across the "three lines of defence"; practice, oversight and audit.

37 A system has been put in place for agencies to report high priority vulnerabilities and security breaches to the GCIO. A more streamlined approach to self-reporting of incident response is also being developed. There are robust arrangements in place for cyber security incidents through both the National Cyber Security Incident Response Plan and the National Cyber Security Centre. There is a need for clearer guidance for agencies on what to do in the case of other incidents relating to lower level breaches. A "no wrong door" policy for agencies is being developed that will leverage existing arrangements in the National Cyber Security Centre and complement the National Cyber Security Incident Response Plan. Clear guidance for agencies will be developed to support this.

38 The NZSIS is leading the establishment of a protective security policy framework for New Zealand. This will update and incorporate SIGS, the NZISM and PSM into one overarching framework and set out clear and mandatory requirements in a way that can be easily accessed by a range of audiences. The objective is to help agencies comply with their obligations and drive a more security aware culture across the State sector. The framework will be supported by monitoring and reporting for assurance purposes, as well as guidance and education for agencies.

Privacy

39 There has been good progress made in providing privacy guidance and support to agencies. Statistics NZ have continued to run the Privacy Working Group and Leadership Forum. These groups have driven the publication of a privacy leadership toolkit, which serves as a mechanism to drive consistency across the State sector through sharing examples of practice.

40 Statistics NZ have also developed a privacy maturity assessment framework, tool and guide which are currently being piloted with a cross-section of agencies. The primary purpose of the tool is to enable agencies to self assess and improve their privacy practices. The self-assessment is based on a capability maturity model and will form a basis for external assurance and/or benchmarking between agencies in the future.

41 There is still further work to do in relation to privacy. This will include:

- Identifying appropriate processes for monitoring and reporting of privacy across the State sector – a separate paper has recently been considered by SEC that would support this work, at the time of writing this is pending Cabinet decision;
- Boosting capacity and capability through expanding the security services panel to include service categories for privacy; and
- Aligning the privacy maturity assessment framework with the protective security policy framework to facilitate integration of privacy and security practice within agencies.

42 By investing further in these areas, a broader, more streamlined framework can be developed and implemented to provide the platform for sustained improvement in privacy and security practice and capability.

Next steps

A streamlined framework to support ongoing compliance and capability

43 Cabinet has tasked the Information Privacy and Security Governance Group with developing a model to enable integrated privacy and security standards, governance, policies and procedures to be consistently applied across the State sector. The group has also been asked to investigate the use of standardised security and privacy reporting across the State sector.

44 All-of-government information management policy is becoming increasingly important with the increasing use of digital channels, greater business process integration and information sharing between agencies.

45 DIA is working with central agencies and other interested agencies to develop an all-of-government information management framework as set out in the ICT Strategy and Action Plan.

46 A streamlined framework for privacy and security will be the first component part of the all-of-government information management framework. This will be delivered through a combination of:

- The *New Zealand Protective Security Requirements*, sponsored by DPMC and led by NZSIS. Implementation of the framework is anticipated in Quarter 2 of 2014, though this is dependent on funding and resource agreements yet to be reached. Cabinet support for the requirements will be sought in early 2014.
- The *Privacy Maturity Assessment Framework*, led by Statistics NZ, and the further work required on privacy outlined above in paragraph 43.
- The *ICT Assurance function*, led by the GCIO, will provide coordinated oversight and delivery of system-wide ICT assurance (including information privacy and security). It will identify areas where interventions may be needed and take action to support agencies where necessary.

47 More information on these initiatives is set out at **Appendix B.**

Plan of Action

48 The plan of action for the Governance Group through to April 2015 is set out in the diagram at **Appendix A**. There are three phases:

March 2013 to September 2013 (this phase is complete)

- Agencies undertook risk assessments of all publicly accessible information systems, security assessments of high risk systems and provided GCIO with a statement of their capability and ongoing improvement plans.
- Guidance and advice was provided to agencies to support capability building.
- The Privacy Leadership Programme led two groups to share expertise and lift capability, developed the privacy leadership toolkit and the privacy maturity assessment framework, tool and guide.
- A model for a streamlined framework to enable sustained improvement to privacy and security was identified.

October 2013 to June 2014

- A common capability security services panel has now been established.
- The privacy maturity assessment framework is currently being piloted.
- A streamlined approach to incident response will be implemented.
- Agencies will report back on progress with their improvement plans and confirm they have completed security assessments of all remaining systems by the end of March 2014.
- The broader framework to enable sustained improvement across privacy and security is under development through alignment of the initiatives outlined in paragraph 46.

July 2014 – April 2015

- A streamlined framework to enable sustained improvement across privacy and security will be implemented with appropriate support and ongoing post-implementation processes.

49 I will receive a progress report on this work programme by June 2014. Over the interim period, the GCIO will continue to engage with agencies to monitor their progress in implementing improvements. In addition, the GCIO ICT Assurance function will provide interventions where appropriate.

50 While agencies are reporting an uplift in practice and understanding of privacy and security, there is still a lot to be done and success will rely on behavioural change at every level of an organisation. The investment required of Chief Executives and Board Chairs to effect this change is likely to be significant.

51 The plan of action seeks to establish a platform for that change; however, continual focus and attention will be required once the framework is implemented, both from Chief Executives and lead agencies, to embed improvements into organisations.

Related initiatives

52 The diagram at **Appendix B** sets out how different initiatives underway across government contribute to the information privacy and security work programme.

53 The outcomes of the information privacy and security programme contribute to the success of a number of initiatives across government, including Cloud computing and Better Public Services result areas (particularly 9 and 10), through building and maintaining public trust and confidence in how the Government manages peoples' personal information.

54 This work programme also contributes to the delivery of a number of actions in the ICT Strategy and Action Plan, including the development of an information

management framework and a mechanism for re-organising capability across the State sector.

55 Governance across related initiatives has been aligned to maximise opportunity wherever possible.

Consultation

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

Financial implications

57 The work required of agencies to meet requirements may be resource intensive.

58 The plan of action will have financial implications for agencies as they will need to engage external suppliers to undertake security assessments and assist them in undertaking their ongoing programmes of improvement. Agencies may also need to engage resource to pilot and implement the privacy maturity assessment framework.

59 The cost of implementing these actions will vary across agencies, depending on their information holdings and their current and planned level of capability.

Human rights implications

60 None.

Legislative implications

61 None

Regulatory impact analysis

62 None.

Gender implications

63 None.

Disability perspective

64 None.

Communications

65 In May 2013, following the initial report on the GCIO Review, Cabinet agreed to publicly release the Cabinet paper and summary of findings. This release was supported by briefings for Chief Executives and the media.

66 To demonstrate the progress being made, I seek Cabinet's agreement to publicly release a copy of this report. The State Services Commission will work with my office and the Government Chief Information Officer on the process for this release.

Recommendations

67 It is recommended that the Committee:

1 **Note** initial improvements in privacy and security over the last six months:

- Agencies have completed security assessments of all high risk publicly accessible information systems.
- Agencies are reporting an uplift in practice and understanding and have plans in place to further improve their capability by March 2014.
- Guidance and advice was provided to agencies to support capability building.
- The Privacy Leadership Programme led two groups to share expertise and lift capability, developed the privacy leadership toolkit and the privacy maturity assessment framework tool and guide.
- Access to market capability is being addressed through the new security services panel, which will help drive consistency, cost effectiveness and transparency.

2 **Note** that a model for a streamlined framework is being developed to enable sustained improvement to privacy and security.

3 **Note** the plan of action for the Information Privacy and Security Governance group through to April 2015.

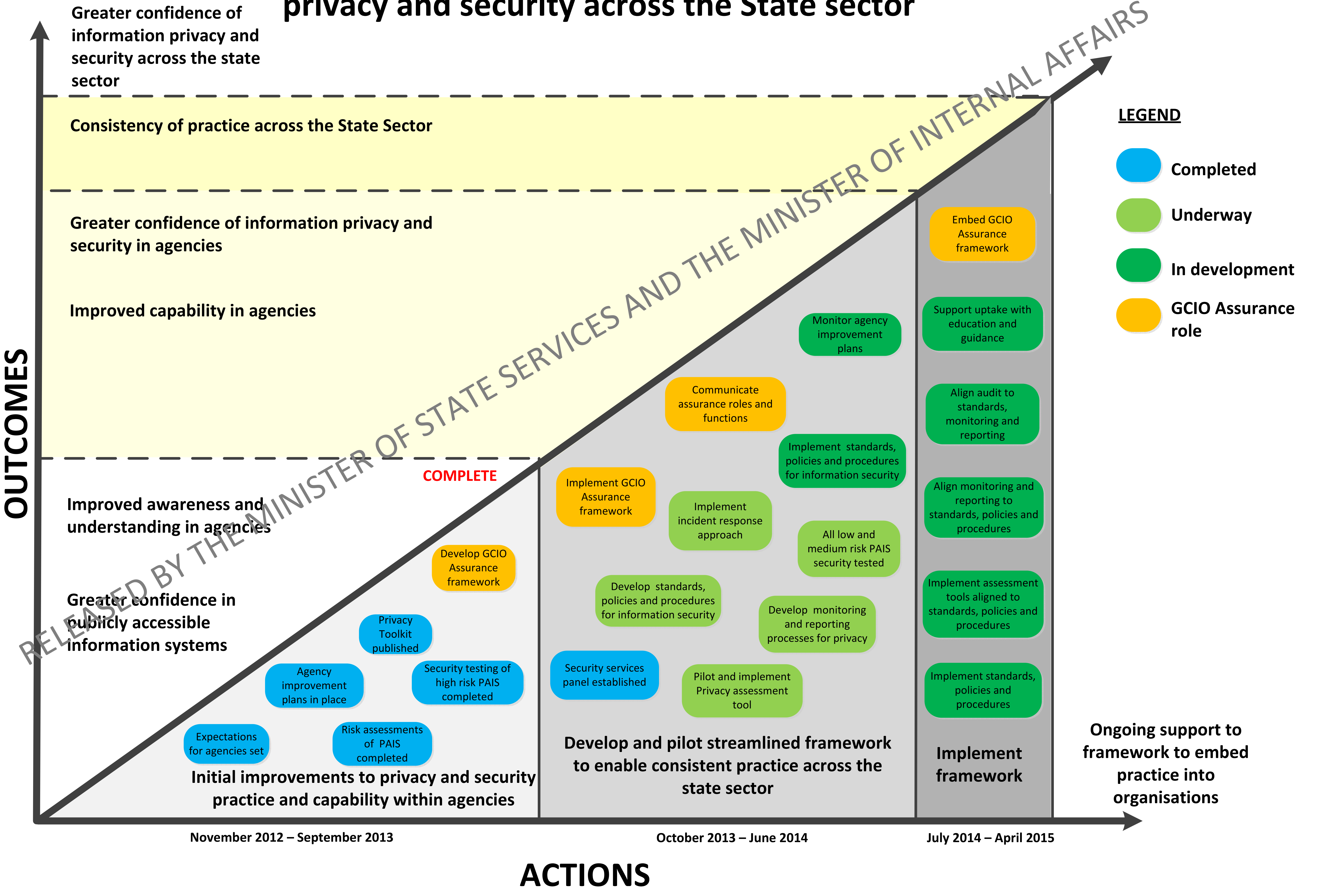
4 **Note** that a number of related initiatives underway across government contribute to the proposed plan of action.

5 **Note** that the Minister of State Services and Minister of Internal Affairs will receive an update on progress against the plan of action by June 2014.

6 **Authorise** the Minister of State Services to release a copy of this Cabinet paper and attachments.

Hon Jonathan Coleman	Hon Chris Tremain
Minister of State Services	Minister of Internal Affairs
____/____/____	____/____/____

Appendix A: Plan of action to improve information privacy and security across the State sector



OUTCOMES

Greater confidence of information privacy and security across the state sector

Consistency of practice across the State Sector

Greater confidence of information privacy and security in agencies

Improved capability in agencies

COMPLETE

Improved awareness and understanding in agencies

Greater confidence in publicly accessible information systems

Initial improvements to privacy and security practice and capability within agencies (November 2012 – September 2013)

- Expectations for agencies set
- Risk assessments of PAIS completed
- Agency improvement plans in place
- Security testing of high risk PAIS completed
- Privacy Toolkit published
- Develop GCIO Assurance framework

Develop and pilot streamlined framework to enable consistent practice across the state sector (October 2013 – June 2014)

- Security services panel established
- Pilot and implement Privacy assessment tool
- Develop standards, policies and procedures for information security
- Develop monitoring and reporting processes for privacy
- Implement GCIO Assurance framework
- Implement incident response approach
- All low and medium risk PAIS security tested
- Implement standards, policies and procedures for information security
- Communicate assurance roles and functions
- Monitor agency improvement plans

Implement framework (July 2014 – April 2015)

- Embed GCIO Assurance framework
- Support uptake with education and guidance
- Align audit to standards, monitoring and reporting
- Align monitoring and reporting to standards, policies and procedures
- Implement assessment tools aligned to standards, policies and procedures
- Implement standards, policies and procedures

Ongoing support to framework to embed practice into organisations

ACTIONS

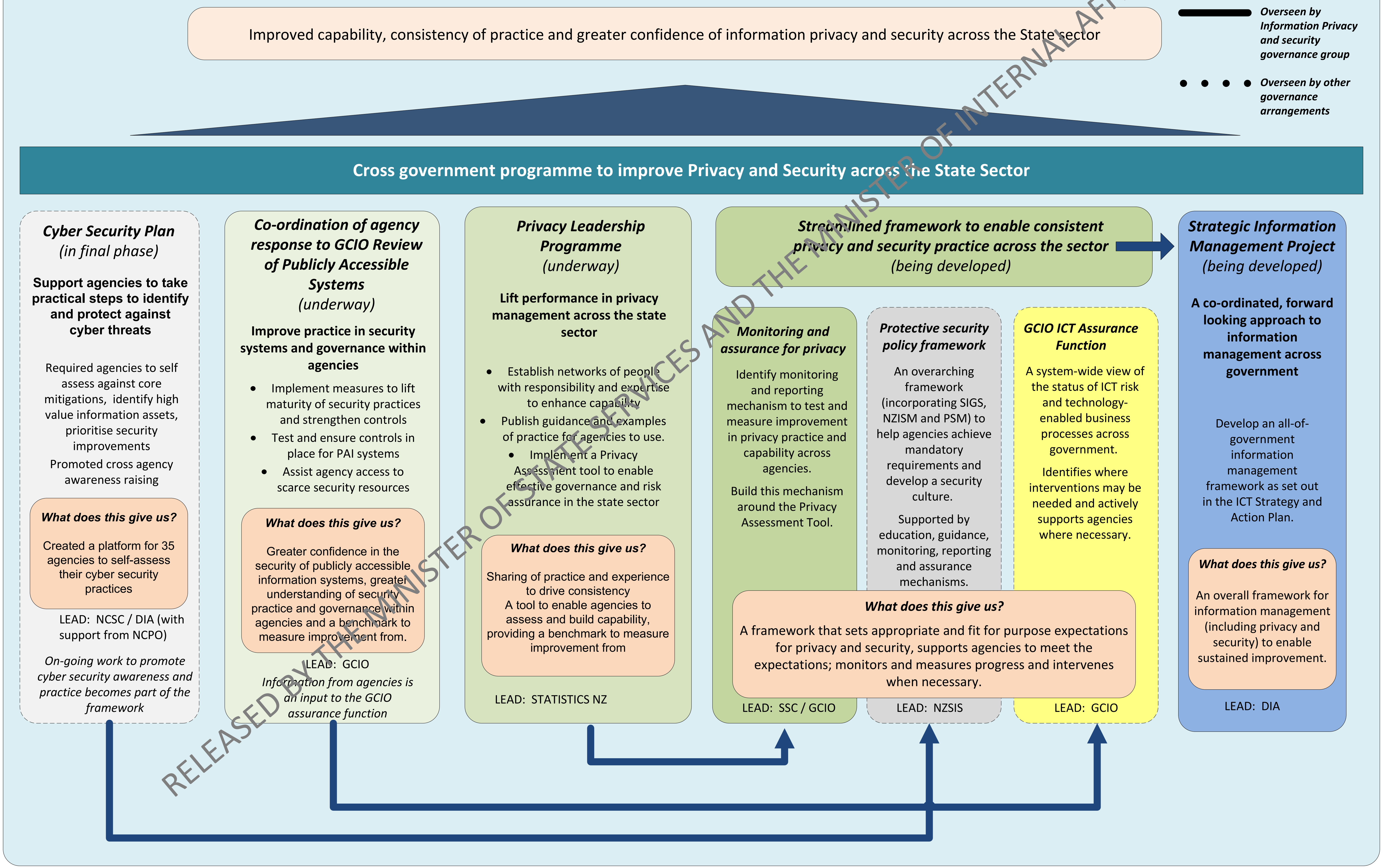
LEGEND

🟦	Completed
🟩	Underway
🟩	In development
🟨	GCIO Assurance role

APPENDIX B

GOVERNMENT PRIORITY – Delivering Better Public Services (effective and efficient)

LONG TERM OUTCOME: To enhance trust in government and confidence in the performance of state sector organisations



Improved capability, consistency of practice and greater confidence of information privacy and security across the State sector

▬ ***Overseen by Information Privacy and security governance group***

● ● ● ● ***Overseen by other governance arrangements***

Cross government programme to improve Privacy and Security across the State Sector

Cyber Security Plan
(in final phase)

Support agencies to take practical steps to identify and protect against cyber threats

Required agencies to self assess against core mitigations, identify high value information assets, prioritise security improvements

Promoted cross agency awareness raising

What does this give us?

Created a platform for 35 agencies to self-assess their cyber security practices

LEAD: NCSC / DIA (with support from NCPO)

On-going work to promote cyber security awareness and practice becomes part of the framework

Co-ordination of agency response to GCIO Review of Publicly Accessible Systems
(underway)

Improve practice in security systems and governance within agencies

- Implement measures to lift maturity of security practices and strengthen controls
- Test and ensure controls in place for PAI systems
- Assist agency access to scarce security resources

What does this give us?

Greater confidence in the security of publicly accessible information systems, greater understanding of security practice and governance within agencies and a benchmark to measure improvement from.

LEAD: GCIO

Information from agencies is an input to the GCIO assurance function

Privacy Leadership Programme
(underway)

Lift performance in privacy management across the state sector

- Establish networks of people with responsibility and expertise to enhance capability
- Publish guidance and examples of practice for agencies to use.
- Implement a Privacy Assessment tool to enable effective governance and risk assurance in the state sector

What does this give us?

Sharing of practice and experience to drive consistency
A tool to enable agencies to assess and build capability, providing a benchmark to measure improvement from

LEAD: STATISTICS NZ

Streamlined framework to enable consistent privacy and security practice across the sector
(being developed)

Monitoring and assurance for privacy

Identify monitoring and reporting mechanism to test and measure improvement in privacy practice and capability across agencies.

Build this mechanism around the Privacy Assessment Tool.

LEAD: SSC / GCIO

Protective security policy framework

An overarching framework (incorporating SIGS, NZISM and PSM) to help agencies achieve mandatory requirements and develop a security culture.

Supported by education, guidance, monitoring, reporting and assurance mechanisms.

LEAD: NZSIS

GCIO ICT Assurance Function

A system-wide view of the status of ICT risk and technology-enabled business processes across government.

Identifies where interventions may be needed and actively supports agencies where necessary.

LEAD: GCIO

What does this give us?

A framework that sets appropriate and fit for purpose expectations for privacy and security, supports agencies to meet the expectations; monitors and measures progress and intervenes when necessary.

Strategic Information Management Project
(being developed)

A co-ordinated, forward looking approach to information management across government

Develop an all-of-government information management framework as set out in the ICT Strategy and Action Plan.

What does this give us?

An overall framework for information management (including privacy and security) to enable sustained improvement.

LEAD: DIA