Timeline of work completed in response to GCIO Review

October 2012	• State Services Commissioner requests that the GCIO undertake an urgent review of publicly accessible ICT systems
December 2012	• **Chief Executives instructed to take immediate action to strengthen information security and privacy controls,** including making an executive-level manager in each agency responsible for robust practices and processes • GCIO report submitted to Ministers
January 2013	• State Services Commissioner considers advice from GCIO and discusses with GCIO • Ministers consider advice
February 2013	• Commissioner briefed Chief Executives in writing on the findings and recommendations of the review • Detailed work programme agreed by GCIO and Commissioner • Cabinet considered review and asked Commissioner and GCIO to suggest additional actions to address agency capability and ensure that the required improvements are implemented as a matter of priority
March 2013	• Cabinet considers and agrees to revised advice • **Release of report deferred to enable further testing to be carried out on systems where vulnerabilities were identified**
28 March	• All 70 agencies in scope of the review instructed by their responsible Minister to commence implementation of work programme • **Implementation of "one month" and "four month" actions begins**
April	• Specialist testing occurs on systems where vulnerabilities were identified, including QA work by GCIO on agencies who have completed their own independent testing
	• In-scope agencies complete "one month" actions: o Provide evidence of detailed risk assessments of publicly accessible systems and email systems; o Consider whether to continue to operate publicly accessible systems and uplift capability; o Report back to GCIO that actions have been undertaken.
17 April	• Information Security and Privacy Governance Group established with responsibility for ensuring: o Recommendations from the review are implemented, measured and sustained; o Security and privacy work across the state sector is well-coordinated.
29 April	• **Time frame for "one month" actions ends – Chief Executives and Chairs report findings to GCIO**
2 May	• All Public Service Departments undertake email risk assessments or high level actions regarding their email systems following EQC breach.
Current	• **Report released** • GCIO establishes a new, mandatory all-of-government security services supplier panel

June	• **Work to set up a single, coordinated point of assurance on Government ICT and strengthen the role of the GCIO released.**
March – July	• In-scope agencies complete "four month" actions and provide GCIO with: o An updated security assessment; o Statement of capability, setting out how they have implemented immediate, "one month" and "four month" actions; o High-level view of ongoing programme to improve security and privacy systems and practices; o Confirmation that they have undertaken all of the prescribed actions; o Any further vulnerabilities identified through security assessments, along with plans to address those vulnerabilities.
29 July	• Timeframe for "four month" actions ends
September	• **Commissioner and GCIO report to Minister of State Services and Minister of Internal Affairs on results of "four month" actions.**