SSC agreement with PIA

A list of the key recommendations made in the Privacy Impact Assessment for the Government Logon Service accepted by the State Services Commission.

To analyse privacy issues with the All-of-government Authentication Programme, the State Service Commission (SSC) has engaged a series of Privacy Impact Assessments (PIAs). The latest PIA, for the proposed Government Logon Service (GLS), was prepared by John Edwards, Barrister and Solicitor. It contains the following key recommendations, which the SSC has accepted:

1. Conduct further PIAs if the system changes such that any participants collect additional personal information.

2. Limit the GLS to government agencies.

3. Comply with the Privacy Act to inform individuals when collecting personal information.

4. Give users security tips, including links to spyware-removal software; and inform them immediately of specific threats.

5. Carefully evaluate business procedures for reissuing or revalidating category-two authentication keys.

6. Develop robust and responsive complaint procedures.

7. Comply with the Privacy Act to respond to requests for access or changes to personal information.

8. Develop policies for retaining information and for closing accounts and disabling keys.

More detailed summaries of each recommendation and response follow.

1. Conduct further PIAs if collecting more information

The current PIA recommends conducting future PIAs if the GLS changes such that service agencies, the common logon service (CLS), key providers, or any other participant in the system collects personal information beyond that defined for the initial implementation. In particular the PIA mentions possible future collection of biometric data.

The SSC agrees that any collection of personal information beyond that scoped for the initial GLS implementation will subject the system to a further PIA; and a critical assumption for this implementation is that the GLS will not collect biometric data.

2. Limit GLS to government agencies

The PIA recommends considering explicitly limiting the GLS to government agencies, for example via cabinet decision, a code of practice, regulations, or an Act of Parliament.

From the beginning, the SSC has intended to limit the initial implementation of the GLS to government agencies. The SSC will confirm this intention with its 2006 Budget recommendations.

Specifically, the 2004 business case SSC submitted to Cabinet on the GLS Initial Implementation described the range of agencies that could use the service as 'all of government'. This term is commonly used to encompass the 'State sector' (all organisations in the annual financial statements of Government, prepared under the Public Finance Act 1989) as well as 'local Government'. The Authentication Programme further restricts GLS users to agencies falling under the jurisdiction of the Ombudsmen Act 1975 and the Privacy Act 1993. (The Offices of the Ombudsmen and the Privacy Commissioner will act as review bodies for the GLS.)

The SSC will confirm these restrictions with upcoming recommendations to Cabinet, for the 2006 Budget round, on GLS roll-out beyond the initial implementation to specifically limit it to those organisations that are listed in Schedule 1 of the Ombudsman Act. If the scope of GLS use ever expands beyond these organisations, the SSC will engage a further PIA and seek further Cabinet approval.

3. Comply with IPP3 (Collection of information from subject)

The PIA recommends developing various means of complying with Information Privacy Principle Three (IPP3) of the Privacy Act [http://www.privacy.org.nz/people/fact3-0.html] which covers an agency's responsibility to inform an individual when collecting their personal information. The PIA recommends educating users about the GLS and its flow of information before issuing a key and whenever critical aspects of the service or its policies change. Further, the PIA recommends requiring GLS users to acknowledge receipt of the information, for example by clicking a link, before the GLS issues them a key.

The SSC agrees that per IPP3 the GLS should inform users about the system and how it collects their personal information, and require them to acknowledge being informed, both before they receive a key and whenever the system changes in any way that may impact on their privacy.

4. Provide security tips

The PIA recommends offering user-friendly 'security tips' in the user-education section of the CLS, including links to spyware-removal software. The PIA further recommends that the GLS immediately inform users, and recommend solutions, for any specific, new threats.

The SSC agrees:

- While the GLS cannot be responsible for the security of devices used to access its service, it will supply up-to-date security tips. These can be presented along with information given as part of IPP3 compliance.

- While developing effective spyware-removal software is beyond the scope of the GLS, it will provide links to appropriate tools for removing spyware (where 'spyware' means malicious software installed on a person's computer system without their active consent).

- While the GLS cannot act as a government security-advisory service for all Internet threats, it will incorporate an active security-monitoring function to detect threats specific to the service; and as indicated it will notify users of those threats and how to deal with them.

5. Evaluate reissue processes for authentication keys

The PIA recommends carefully evaluating the business procedures for re-issuing or re-validating identities with category-2 authentication keys in future implementations, so as to avoid introducing any weak links in the security chain.

The SSC agrees that before introducing other key types, including two-factor authentication keys, the programme will carefully evaluate business procedures for controlling the re-issue and re-validation of existing keys.

6. Develop complaint procedures

The PIA recommends developing robust and responsive complaint procedures for the GLS, including:

- appointing a Privacy Officer

- issuing memoranda of understanding (MOUs) with service agencies

- requiring service agency cooperation with any investigation of allegations of misuse of keys or data.

The SSC is developing detailed complaint procedures (along with other operational procedures) for the GLS. The SSC Privacy Officer will serve as Privacy Officer for the GLS since it is a service of the SSC. The GLS will help service agencies investigate allegations of key misuse promptly and at no cost or inconvenience to users.

7. Comply with IPP6 (Access to personal information)

The PIA recommends developing means to comply with IPP6 [http://www.privacy.org.nz/people/fact3-0.html] of the Privacy Act. IPP6 which covers a person's right to access and correct held information. In particular, the PIA notes the need for identify-verification procedures for people requesting access or changes to their information.

The SSC is developing procedures for users to access and change their information in line with privacy legislation. Before the GLS responds to any such request, users will need to verify their identity (as they would for any offline customer support).

8. Develop policies for retaining information, closing accounts, and cancelling keys

The PIA recommends developing policies for how long to retain transaction logs, how to treat apparently inactive accounts, and how to cancel keys.

The SSC is developing policies and procedures to comply with privacy legislation and 'good-practice' security management. The GLS website will include information on how the system retains information, closes inactive accounts, disables keys, and lets users leave the system.