Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Feb. 8, 2013

Statement from B.C. Information and Privacy Commissioner on the BC Services Card

The BC Services Card is the first program of its kind in Canada. The BC Government states the program's ultimate aim is to provide secure authentication of citizens seeking access to government services. By design, this program will collect, use, and disclose the personal information of virtually every British Columbian. And future phases could enable multiple government services to be accessed online.

I understand that citizens want convenient and efficient access to government services, and that in order to provide these services, government must be able to securely authenticate users. However, it is critical that the BC Services Card be built with robust privacy protection by design.

My office has completed a review of Phase 1 of the BC Services Card. This phase is limited to the enrollment of individuals and issuance of the card, built around a provincial Identity Assurance Service. Our review included an examination of the legal authorities for sharing data, and a review of the technological systems and security measures in place to protect personal information.

We have determined that the issuance of the BC Services Card and the initial systems needed to support it meet legal requirements. However, I am making several recommendations to enhance the existing privacy and security provisions.

Phase 1 represents only the first step in the program; Phase 2 will be a significantly larger step that brings with it considerable risks to personal privacy, in that there is the potential for data linkages to connect an individual's discrete activities across multiple platforms. My office will continue to watch vigilantly as the phases move forward. We will conduct quarterly reviews over the next year, at a minimum, to verify that proposed security measures outlined in Phase 1 are being implemented, and to provide a thorough review of the proposed functionality of Phase 2.

I remain deeply concerned that the public has not been consulted about the BC Services Card program as a whole. Given the program's profound reach and the

amount and type of personal information involved, it is critical that citizens are included in the dialogue.

I am recommending that government conduct a fulsome public consultation with British Columbians before the BC Services Card program proceeds to Phase 2. At a minimum, government must explain its long-term vision for the card, the potential benefits to be gained, as well as the risks. The public must be given an opportunity to have their say. Solutions that government proposes to address these risks must also be subject to scrutiny, by both the public at large and by those with technical knowledge in the field.

I have shared my views and recommendations with government in a detailed letter, which I am releasing today in the spirit of transparency, and as a first step towards public engagement on the BC Services Card.

-30-

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

February 05, 2013

Kim Henderson
Deputy Minister
Ministry of Citizens' Services
and Open Government
PO Box 9440 Stn Prov Govt
Victoria BC V8W 9V3

Dear Kim Henderson:

Re: BC Services Card Phase 1 Review

I am writing to convey my office's views on the privacy and security framework for Phase 1 of the BC Services Card Program.

This first phase of the program is the enrolment and issuance of a new BC Services Card built around a provincial Identity Assurance Service ("IAS") and the use of IAS to update the Health Client Registry.

There will be three versions of the card: one combined with a driver's license, one standalone card with a photograph, and one which does not contain a photograph. The Insurance Corporation of British Columbia's ("ICBC's") front-counter identity-proofing services and facial recognition technology will be utilized to enrol BC residents with combined and standalone cards and Health Insurance BC will enrol individuals with the non-photo card.

The BC Services Card will contain an integrated circuit chip. Future phases of the program will enable additional government services to be accessed online and in-person by utilizing this chip to authenticate an individual's identity.

I understand that, increasingly, British Columbians want to access services online, and that in order to provide online services, government agencies need to securely authenticate users. However, it is imperative that such identity validation services be built with robust personal privacy protection as a fundamental design element, which is the focus of my office's mandate.

Mail: PO Box 9038, Stn Prov Govt, Victoria BC V8W 9A4
Location: 4th Floor, 947 Fort Street, Victoria BC
T. 250 387 5629 F. 250 387 1696
Toll free through *Enquiry BC* 800 663 7867 or 604 660 2421 (Vancouver)
W. www.oipc.bc.ca

I also appreciate you are designing the first program of its kind in Canada, and therefore there is limited experience to draw upon from other jurisdictions. From my point of view, this reinforces the need to be vigilant regarding personal privacy issues, since this program involves the collection, use and disclosure of the personal information of nearly every British Columbian.

Scope of the OIPC Review

I am charged under s. 42 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") with commenting on the implications for protection of privacy of proposed programs by public bodies.

More specifically, s. 69(5.2) of FIPPA directs me to review and comment on privacy impact assessments ("PIAs") developed for a common or integrated program such as the BC Services Card.

Consistent with this mandate my review of Phase 1 of the BC Services Card encompasses the establishment of this integrated program, the legal authorities for the collection, use, and disclosure of personal information, and the technological systems and security measures in place to protect the personal information of BC citizens.

We have reviewed PIAs from each of the partners [the Ministry of Citizens' Services and Open Government ("CITZ"), the Ministry of Health ("MoH"), and the ICBC].

We also reviewed documentation pertaining to the system architecture, methods for securing personal information in transit and at rest, Security Threat Risk Assessments ("STRAs"), and the Integrated Program Agreement ("IPA") and Information Sharing Agreement. Because of the abbreviated time for review, we have not assessed those systems that already exist at ICBC or at the Health Client Registry of MoH.

What follows is a description of the scope of my review, recommendations for government actions going forward, the actions my office will take as part of an ongoing review of the program and a major recommendation to enhance the confidence of citizens in this major initiative.

Legal Authority for the Program

This program is enabled by legislative amendments to FIPPA in November 2011 that established the legal authority for collection and disclosure of personal information by the designated Provincial Identity Information Services Provider ("PIISP"). In addition, amendments to the *Motor Vehicle Act* ("MVA"), and the *Medicare Protection Act* ("MPA") authorize ICBC and MoH to partner with CITZ to develop and implement the BC Services Card.

As stated in our letter of September 12, 2012 we agree that the collection, use, and disclosure of personal information between the three partner public bodies, as described in the PIAs, is authorized by these provisions of FIPPA, the MVA and the MPA.

IAS Access and Audit Logs

The PIISP will operate the IAS, which will collect and store the personal identity information of residents enrolled in the BC Services Card program. In the first part of Phase 1 of the program, this will be limited to the personal information of residents who are enrolled in the Medical Services Plan (MSP). In November 2014, scheduled amendments to the MVA Identification Card Regulation will expand BC Services Card enrolment to include non-recipients of MSP.

Personal information will be retained in the audit logs for the Task Information Management System ("TIMS"). We understand that at this time, IAS will be retaining TIMS logs indefinitely. We will monitor the use of these logs to assess the data flow between ICBC and IAS.

- We recommend that CITZ develop a retention policy for these access and audit logs that includes a destruction schedule.

System Design and Security

Given the amount of personal information that will be collected, used, and disclosed in the program, it is imperative that the information sharing pathways and associated storage systems are secure. Section 30 of FIPPA requires that public bodies must make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information in their custody and control. I have the following observations and recommendations for the security of personal information.

Our analysis of the program's systems architecture and security measures considered both the security of information "in transit" (communication pathways between the partners), and "at rest" (held by the partners), including technological and human vulnerabilities.

The transfer of personal information between the IAS and MoH is protected by 128 bit encryption, which meets the minimum standard for such transfers. However, government's own standards recommend the use of 256 bit encryption where communications are to occur over the Internet.

- We recommend that the higher level of 256 bit encryption be employed to protect personal information in transit.

Personal information can be further protected by the use of 'payload' encryption for information in transfer. This will provide a second layer of protection against a data breach in the event the transfer is compromised.

- We recommend that the transfer of personal information be protected by payload encryption.

Privacy Management Programs

All public bodies that collect, use, and disclose personal information must have a privacy management program in place to protect that information. With a program of this scope comes significant risk of unauthorized access, abuse, and loss of data. This risk will inevitably increase as additional public bodies sign-on to access the IAS. My expectation is that any new parties that are added to the IPA or that utilize the authentication facility of the IAS will have robust privacy management programs in place.

The integrated program agreement and government policy requires that future partners in this initiative provide privacy impact assessments, and information sharing agreements. In my view, this "paperwork of privacy" although important, is insufficient to assure British Columbians that their personal information is protected. Public bodies need to stand ready to demonstrate that policies, privacy and security controls are implemented, actively reviewed, audited and reported on by management. To that end I am asking government to execute a letter of understanding with my office stating that it will require any new parties and clients to the program to have the necessary elements of a privacy management program in place. To assist in this work, I will be issuing a directive that defines the elements of such a program, as I have done for private sector organizations.

- New parties and clients to the BC Services Card should be required to demonstrate the adequacy of their privacy management programs to Citizens' Services before entering into this initiative.

Ongoing OIPC Review

Government has made a series of commitments about the privacy and security of Phase 1 of the program. Given the importance of this initiative, I think it incumbent upon my office to follow up on these commitments by conducting quarterly audits of the BC Services Card program for at least the first year of its operation to assess whether the systems are constructed as set out in the PIAs, and are functioning in a privacy protective and secure manner. Our audit will include ongoing review of STRAs and any changes to the systems and security architecture.

Our ongoing review of the BC Services Card program will include assessments of:

- Employee training manuals that have been developed for the BC Services Card initiative to better understand how internal attacks may be mitigated and managed.

- Changes, if any, to the Integrated Program Agreement between the three partners.

- New PIAs and information sharing agreements for onboarding public bodies to the BC Services Card as subsequent phases of the program evolve.

- Government's tool to assess the readiness for programs and agencies that wish to access BC Services Card based services in future phases (the "on-boarding kit"). I understand that you will be consulting with my office on necessary elements of a privacy management program that programs and agencies must have in place prior to on-boarding.

- Notice materials required in the event of any new collection of personal information in this phase.

- The program's Disaster Recovery Planning to determine what policies and procedures are in place to mitigate a Dedicated Denial of Service type of attack, and what transpires in the event IAS is unable to provide identity authentication services.

Major Recommendation for Public Consultation

I recognize that providing secure and assured identity transactions with government is an important public policy goal. However, as the BC Services Card program will eventually contain the personal information of nearly every British Columbian, this goal must be achieved through a process of meaningful public consultation.

Government transparency promotes accountability to its citizenry. Given the benefits and risks associated with a program of this magnitude, government should consult directly with citizens about the vision, scope, privacy risks and safeguards of this initiative.

The BC Services Card program raises significant concerns regarding misuse of personal data, such as unauthorized access, profiling, and function creep. Solutions that government proposes to address these risks should be subject to scrutiny by both the public at large and by those with technical knowledge in the field.

I have expressed my concern that the government has chosen not to consult the public broadly in the development of Phase I of the program. I believe that future phases of this program will be jeopardized if the government does not build public trust, which comes from sharing information about the objectives of the program, and privacy risks.

Conclusion

I appreciate government's cooperation with my office's review of Phase 1 of the BC Services Card program.

In our review of the documentation relating to Phase 1, we found the program has designed privacy and security considerations appropriately, subject to the recommendations contained herein. We will monitor implementation to provide assurance that what has been designed, operates as planned.

I sincerely recommend that government undertake a fulsome process of public consultation on this program to ensure public knowledge and trust in its benefits and potential risks to personal privacy, specifically that such consultation be undertaken prior to phase 2 of the program.

Sincerely,

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia