Office of the
Chief Electoral Officer
of Ontario

Bureau du directeur
général des élections
de l'Ontario

July 17, 2012

The Honourable Dave Levac
Speaker of the Legislative Assembly
Room 180, Legislative Building, Queen's Park
Toronto, Ontario M7A 1A2

Dear Mr. Speaker,

I am writing to notify you about a privacy breach that impacts individuals who, on October 6, 2011, were resident in certain Ontario electoral districts. This matter is not in any way related to the October 2011 general election and does not in any way impact its outcome.

I take this matter extremely seriously and I sincerely apologize to all Ontarians for the worry that this may cause them.

The privacy breach concerns copies of personal information stored on two USB keys that cannot be located.

We have undertaken both a rigorous search as well as a full internal investigation to completely review the matter. I engaged Gowlings to initiate and guide an independent investigation, supported by INKSTER Incorporated, a forensic security specialist firm.

I am submitting to your office, so it may be put before the Legislative Assembly, a report entitled "Preliminary Report Regarding the Privacy Breach at Elections Ontario", prepared by Gowlings. The report outlines what happened and the advice and recommendations that I have received to date.

I have reported this matter to the Ontario Provincial Police (OPP). The OPP is investigating. I have also asked the Office of the Information and Privacy Commissioner of Ontario to assist Elections Ontario in a full review of our privacy policies and procedures and to consult with us in ensuring that this circumstance is not repeated.

Finally, since receiving the Gowlings "Preliminary Report Regarding the Privacy Breach at Elections Ontario", I have immediately directed the following:

- An immediate and comprehensive review of all Elections Ontario policies, processes, procedures and protocols related to the privacy, management, protection and custody of voter information including staff orientation, training, management oversight and accountability and audits.

- An immediate and comprehensive review of Elections Ontario's Technology strategic framework, infrastructure and management policies and oversight.

These activities are separate from the review conducted by the Office of the Information and Privacy Commissioner. Both will be undertaken by external expert resources directly accountable to me.

51 ROLARK DRIVE • TORONTO, ONTARIO M1R 3B1 • VOICE:(416) 326-6300 TTY: 1-888-292-2312 FAX: (416) 326-6201
51, PROM. ROLARK • TORONTO (ONTARIO) M1R 3B1 • VOIX: (416) 326-6300 ATS: 1-888-292-2312 TÉLÉ: (416) 326-6201

I will be tabling a comprehensive report to the Legislative Assembly about this matter by year end, summarizing the outcomes of the Gowlings and INKSTER Incorporated investigation, the OPP investigation and the Information and Privacy Commissioner's review.

Again, please accept my sincere and personal apology. At your convenience, I will be pleased to meet with you to answer any questions that you may have.

Sincerely,

Greg Essensa
Chief Electoral Officer

REPORT REGARDING THE PRIVACY BREACH AT ELECTIONS ONTARIO

Gowling Lafleur Henderson LLP
K. Lynn Mahoney

July 2012

I. Introduction

Gowlings has been retained by the Chief Electoral Officer to review and report on the circumstances surrounding the loss from an Elections Ontario facility of two USB drives containing data including elector information, which occurred on or about April 26, 2012.

To conduct this review and provide this report we have been working with senior staff and management at the office of Elections Ontario and also with the professional security consulting firm, Inkster Incorporated.

This report describes the nature and scope of this privacy breach, what Elections Ontario has been advised about the risk this poses to electors, and recommendations for steps to be taken.

II. Background

Mandate of the Chief Electoral Officer

The Office of the Chief Electoral Officer, known as Elections Ontario, is a non-partisan agency of the Legislative Assembly of Ontario that operates under the direction of the Chief Electoral Officer, an officer of the Legislative Assembly. Permanent Staff assist the Chief Electoral Officer in carrying out his responsibilities, which include the organization and conduct of general elections and by-elections in accordance with the provisions of the *Election Act,* the *Election Finances Act,* and the *Representation Act*. Under the *Election Act*, the Chief Electoral Officer is responsible for the maintenance of the Permanent Register of Electors for Ontario, which sorts by Electoral District where every eligible voter in Ontario lives.

Managing Elector Information

The 2011 General Election in Ontario resulted in the election of a minority government. Accordingly, Elections Ontario was required to put into place, as quickly as possible, all arrangements, including obtaining the documentation and forms necessary to run a subsequent election, on short notice, should circumstances dictate. At the same time, Elections Ontario was involved with the processing of the election documents from the 2011 General Election, which had been returned along with all other supplies and materials to Elections Ontario by the Returning Officers for each of the 107 provincial Electoral Districts.

Elections Ontario's permanent facilities are located at 51 Rolark Drive, Scarborough, Ontario. The Rolark facility provides offices and work stations for Elections Ontario employees (both permanent and part-time), as well as secure storage for election documents and related supplies and materials.

The Rolark facility did not have adequate space to provide storage for the new documents, supplies and materials, which had been ordered in preparation for a possible election in the near term, as well as the documents that had been returned to Elections Ontario following the 2011 General Election. As a result, additional storage space was leased near Elections Ontario, on Birchmount Road, in Scarborough, Ontario to store the election documents from the 2011 General Election.

One post-election task that Elections Ontario undertakes is to update the Permanent Register of Electors for Ontario using the information obtained by elections officials during the election with respect to who should be deleted, transferred or added to the voters list for an Electoral District. Elections Ontario also centrally records who voted by reviewing which electors were marked as having voted or "struck-off" on the Polling Day List of Electors by polling officials. These lists are returned to Elections Ontario by Returning Officers.

Post-election tasks are performed during the "Strike-Off Project" by Elections Ontario Staff who use hand held scanning devices to scan the barcode beside the name of each elector who is recorded to have voted on the Polling Day List of Electors. The information is scanned into an electronic database with a separate file for each Electoral District that is used to update the Permanent Register for Electors in Ontario.

The Strike-Off Project work was being done in the facility on Birchmount Road. Elections Ontario contracted with a bonded alarm security company to install an electronic alarm system in the facility. To gain access to the facility, the door had to be unlocked with a key and a unique code entered into the alarm system. A record was kept of those staff members provided with a key and given the alarm code. All of the staff working on the project took an oath or affirmation of secrecy.

Elections Ontario provided laptops to the staff involved in this project, each protected by a password. User IDs were assigned to each of the 17 laptops. The laptops were not networked and were not connected to the Elections Ontario network, therefore, two USB drives were to be used for the purpose of transferring information amongst the laptops in the facility.

The Elections Ontario Permanent Register and List of Electors Privacy Policy stipulates that the USB drives were to be encrypted and password protected, stored securely in a locked location, with access to both USB drives confined to specified personnel.

III. Privacy Breach

Chronology of Events

At the end of the day on April 23, 2012, the Strike-Off Team at the Birchmount facility was advised not to report to work on April 24, 2012 as mold had been detected in the facility and needed to be removed.

On April 25, 2012, Elections Ontario Permanent Staff attended at the Birchmount facility to perform some quality control work while the Strike-Off Team was off work. The two USB drives were found to be unsecured. Following the use of these USB drives, the Staff left them unsecured in the facility. Neither of the USB drives was encrypted or password protected.

On April 26, 2012, Elections Ontario Permanent Staff returned to the Birchmount facility to continue working on quality control. At approximately 3 p.m. it was discovered that the two unencrypted USB drives were missing. No other Elections Ontario property, including the laptop hardware, was missing. The staff commenced a search for the USB drives, which continued for the remainder of that day and into the following day, but did not result in the recovery of the USB drives.

The fact that the USB drives were missing was reported to senior staff at Elections Ontario on April 27, 2012.

Nature of the Information

The information on the USB drives contained Electoral District files, specifically information about persons eligible to vote who lived in particular Electoral Districts in October 2011. The information included people's full name, gender, birth date, and address as well as administrative codes used solely for election purposes and any elector information updates provided during the last writ period. The information may also have included whether or not the person voted in the October 2011 General Election. It would not have included any information about how they voted.

The information contained on the USB drives did not include the following information:

- Social insurance numbers
- Ontario Health card numbers
- Drivers licence information or numbers
- Telephone numbers
- Credit card or banking information
- Any other information provided by electors during the 2011 General Election to confirm their identity or residence

Scope of the Information

The staff who last worked with the USB drives on April 23 and 25, 2012 advised that it is likely there was information for 3 Electoral Districts on one USB drive and information for 17 to 22 Electoral Districts on the other USB drive. There were 49 Electoral District files being worked on simultaneously, with information relating to just over 4 million electors.

Despite extensive forensic investigation and analysis, it has to date been impossible to determine with absolute certainty which of the approximately 25 Electoral District files were stored on the USB drives. Attached as Appendix A is a list of these 49 potentially affected Electoral Districts.

Risk Assessment

Risk of Unauthorized Access

While the USB drives were not encrypted, the data itself can only be accessed in an intelligible form by internal Elections Ontario software or specialized commercial software applications.

Risk of Identity Theft of Information Obtained Through Unauthorized Access

There is no evidence that electors' personal information has been improperly accessed. However, it is recommended that electors, who lived in these Electoral Districts in October 2011, monitor and verify their transaction statements with governments, financial institutions, businesses, and other institutions to detect any unusual activity. If any suspicious activity is detected, contact should be made immediately with these institutions.

IV. Immediate Response and Internal Investigation

Response

Immediately following the discovery of the loss of the USB drives, procedures reinforcing the Elections Ontario Permanent Register and List of Electors Privacy Policy were put into effect and staff were trained on them. These measures included the adoption of new user names and passwords on the laptops, the adoption of passwords on the USB drives and access to the USB drives being restricted to Permanent Staff members at all times.

Internal Investigation

Immediately following this incident, persons with access to the facility were questioned. The event records for the security system were reviewed by the alarm security company at Elections Ontario's request.

A detailed questionnaire was administered to all persons with access to the facility to investigate the circumstances regarding the loss.

The survey results did not furnish any additional information that was helpful in explaining how the USB drives were lost.

Conclusions

When the decision was made to use the USB drives for the transfer of information, procedures to implement the Elections Ontario Permanent Register and List of Electors Privacy Policy within the Birchmount facility were established to ensure data security and safety. These procedures were explained to the staff however it was found that they were not observed. Neither USB drive was encrypted or password protected nor were they stored safely and securely.

At the conclusion of the internal investigation, it was recommended that external professional security and computer forensic consultants be retained to assist in determining the nature and extent of the security breach before the public could be advised.

V. Third Party Review

Upon the conclusion of the internal investigation, on May 25, 2012 the Chief Electoral Officer retained professional security consultants from Inkster Incorporated to review the circumstances surrounding this situation.

Inkster's Preliminary Findings

Inkster Incorporated's inquiries indicated the Strike-Off Team did not have the software to encrypt the files and make them unreadable without the proper password and software. Subsequent inquiries clarified that encryption software was available on the USB drives but had not been activated.

As had been disclosed in the internal investigation, while the Strike-Off Team was instructed to use the password protection offered by the Windows zipping or compression software, the Team was not regularly zipping and password protecting the

files on their laptops as required by the Elections Ontario Permanent Register and List of Electors Privacy Policy.

Inkster Incorporated confirmed the findings of the internal investigation that staff were using the USB drives to store non-password protected data as a back-up of data on their laptops. Although the laptops themselves were password protected, the files on the laptops were not encrypted or password protected.

While the Strike–Off Team was assigned individual User IDs to perform their tasks on selected laptops, all staff members shared the same basic default password before April 26, 2012. While users were prompted by the system to change the default password, the change process was not electronically enforced as the laptops were standalone and no password expiration date was programmed. Inkster Incorporated concluded that having the same password for all staff was a poor practice and a security risk to information contained on the system.

While transfer and back-up procedures were apparently repeatedly reviewed with the staff, there were no written instructions provided specifying the deletion of the data on a USB drive. Although staff were verbally told to keep the USB drives secured when not in use, consistent with the Elections Ontario Permanent Register and List of Electors Privacy Policy, that protocol was not followed.

Inkster's Recommendation

Throughout the work conducted by Inkster Incorporated a number of observations were made to Elections Ontario to address issues of information control and storage in the immediate term. Inkster was advised by Elections Ontario that these observations would be acted on as quickly as possible.

Inkster Incorporated recommended that a thorough and complete threat, risk assessment and security review be conducted at Elections Ontario to enhance the profile of security within the organization and to ensure that appropriate risk management policies, procedures and safeguards are in place to protect and secure elector information. This threat, risk assessment and security review should include:

- Development of enhanced training programs to assist Elections Ontario staff by reinforcing the importance of the secure treatment and storage of elector information and the steps to be taken in the event that a loss of private information is suspected including the reporting of any suspected loss to the Privacy Commissioner of Ontario and/or the Ontario Provincial Police as appropriate;

- Examining the need to establish a position within Elections Ontario responsible for the security at Elections Ontario, coordination of subsequent security

assessments and reviews as well as internal investigations should they be necessary;

- Development of a protocol to assist Elections Ontario staff in the proper conduct of internal investigations as and when necessary, the content of which should include guidance in the proper conduct of internal enquiries, the taking of statements as well as the preparation of notes and reports;

- Establishment of procedures for the correct and timely treatment of "whistle blower" complaints/concerns;

- In consultation with the Privacy Commissioner of Ontario, development of protocols to guide Elections Ontario staff in any actions to be taken and reporting of any suspected loss of personal elector information in a timely and effective manner;

- Training of technical services staff in respect of appropriate safeguards for electronic data, the recovery of such data if required, and include an audit/review process to ensure that all safeguards are implemented and that rules are being followed;

- Overall periodic review/audit by an expert external to Elections Ontario of the security measures in place at Elections Ontario to ensure that measures are up to date in respect of the current risk/threat environment, are effective and are being followed by Elections Ontario staff.

VI. External Investigations

Based on their review, which has not yet concluded, Inkster Incorporated recommended on June 13, 2012 that the Chief Electoral Officer refer the matter to the Ontario Provincial Police for investigation, which he did immediately. The OPP are currently conducting an investigation.

On July 5, 2012, the Chief Electoral Officer invited the Information and Privacy Commissioner to review this matter. The Information and Privacy Commission are currently conducting an investigation.

Appendix A

The following is a list of those potentially affected Electoral Districts and the number of electors:

	Electoral District Name	Number of Electors
1.	Ajax—Pickering	92745
2.	Algoma—Manitoulin	52919
3.	Ancaster—Dundas—Flamborough—Westdale	88080
4.	Brampton West	115431
5.	Brant	94717
6.	Bruce—Grey—Owen Sound	75809
7.	Burlington	90964
8.	Davenport	68998
9.	Don Valley East	69851
10.	Don Valley West	82533
11.	Essex	89549
12.	Etobicoke Centre	81413
13.	Etobicoke—Lakeshore	87390
14.	Etobicoke North	62472
15.	Haliburton—Kawartha Lakes—Brock	89830
16.	Halton	128643
17.	Hamilton Centre	79524
18.	Kingston and the Islands	95966
19.	Kitchener Centre	80170
20.	Kitchener—Conestoga	87992
21.	London—Fanshawe	75165
22.	London North Centre	91638
23.	London West	93852
24.	Mississauga South	78746
25.	Mississauga—Streetsville	87297
26.	Nepean—Carleton	110662
27.	Newmarket—Aurora	92231
28.	Nickel Belt	62276
29.	Nipissing	59481
30.	Northumberland—Quinte West	93720
31.	Ottawa South	87766
32.	Ottawa—Vanier	81712
33.	Ottawa West—Nepean	82187
34.	Peterborough	91908
35.	Pickering—Scarborough East	78835
36.	Prince Edward—Hastings	86304
37.	Sarnia—Lambton	78646
38.	Sault Ste. Marie	59698
39.	Scarborough—Agincourt	73583
40.	Simcoe—Grey	97272
41.	Simcoe North	89474
42.	Stormont—Dundas—South Glengarry	75975
43.	Timiskaming—Cochrane	50554
44.	Timmins—James Bay	49723
45.	Toronto Centre	95466
46.	Whitby—Oshawa	102672
47.	Windsor West	82773
48.	York Centre	71531
49.	York West	58255
Total:		**4054398**