Information and Privacy Commissioner/Ontario
Commissaire à l'information et à la protection de la vie privée/Ontario

News Release **July 31, 2012**

Commissioner Cavoukian's investigation finds systemic failures at Elections Ontario – paving the way to the largest privacy breach in Ontario history

Massive breach could have been avoided if personal data had been encrypted

TORONTO, ON – Elections Ontario's loss of two USB keys containing the unencrypted personal information of as many as 2.4 million voters can be traced back to the agency's failure to systemically address privacy and security issues, said Information and Privacy Commissioner Dr. Ann Cavoukian today, in releasing the findings of her investigation. In reality, four million people are impacted: Elections Ontario could not identify which of the 20 to 25 electoral districts from a group of 49 were involved, thus increasing the number of affected Ontarians. As a precaution, Ontarians in the identified electoral districts should remain alert and monitor their bank accounts and credit card statements, and alert their financial institutions if they notice any suspicious activity.

To provide some context, the October 2011 provincial election resulted in a minority government, requiring Elections Ontario to prepare for the possibility of another snap election. The agency's headquarters did not have the capacity to simultaneously store materials for a potential election and conduct their required post-election update of the Permanent Register of Electors for Ontario, known as the Strike-off Project. As a result, the decision was made to conduct the data update project at a leased warehouse near their headquarters. The two USB keys in question were used to transfer elector data between members of the project working at the warehouse. Contrary to agency policy, the information transferred via the USB keys was not encrypted.

"Personal information is the currency in which Elections Ontario trades. I am astounded at the failure of senior staff to address the security and technological challenges posed by the decision to locate the project off-site," said Commissioner Cavoukian. "Ultimately, at the root of the problems uncovered in the course of my investigation was a failure to build privacy into the routine information management practices of the agency."

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

On April 26, staff at Elections Ontario realized that the two USB keys in question had gone missing. The incident was reported to senior management and an extensive internal investigation was launched. When an extended search did not find the keys, the agency retained external legal counsel to advise and initiate an independent investigation, supported by a forensic security specialist firm. This matter was subsequently reported to the Ontario Provincial Police, who are conducting their own independent investigation. Commissioner Cavoukian was not notified until July 5, at which time she advised Elections Ontario to notify the public as soon as possible. The notification took place through a media conference on July 17 and newspaper ads in major dailies on July 18 and 21.

Over the course of the investigation the Commissioner learned that the Strike-off Project had resumed its work on April 30, again without adequate measures to ensure the privacy and security of electors' personal information. While a number of measures were implemented to address the security deficiencies in the project, these measures were totally inadequate and failed to address the glaring privacy risks raised by the loss of the keys. Most significant, the project resumed by using a replacement set of USB keys. While these keys possessed an encryption functionality, it was never activated! Frontline staff remained ill-informed of the meaning of encryption, or how to deploy the encryption capabilities. Alternatives to the use of the keys were slow in being requested and implemented.

"Given the experience of the previous week, it is truly surprising that the Strike-off Project would have continued using USB keys. Even more egregious is the fact that the data on the keys continued to be unencrypted. Elections Ontario's efforts to continue the Strike-off Project in this manner were totally inappropriate in light of the breach that had just occurred," said the Commissioner.

The investigation also examined the policies and procedures in place at Elections Ontario to protect the privacy and security of electors' personal information. While there appeared to be a general recognition at the agency of the importance of privacy and security, for the most part, concerns about how personal information was managed tended to be directed to Elections Ontario's external stakeholders, who were the recipients of the information. The need for internal vigilance to protect personal information at the agency itself was not supported by robust policies and procedures.

"What is particularly discouraging was the discovery that the privacy and security of personal information was not part of any training programs that were offered to staff – despite the nature of the information in the custody and control of Elections Ontario. Needless to say, this is completely unacceptable," added the Commissioner. "I am committed to working with the Chief Electoral Officer to ensure that the privacy of Ontario voters is embedded into the agency's operations, not by chance, or by disaster, but by design."

The irony of such a massive breach occurring in Ontario is the fact that *Privacy by Design* – unanimously passed as an International Privacy Standard in 2010, originated in Ontario! Privacy by Design is now being followed all around the world, except, it would appear, in Ontario.

As a result of the investigation, the Commissioner has recommended that Elections Ontario take concrete steps in three areas to enhance the protection of personal information:

- **Policies, Practices and Procedures** – Retain the services of an independent third party to audit Elections Ontario's current privacy and security policies and procedures, as well as to develop an agency-wide privacy policy, including the requirement for any personal information stored on mobile devices to be encrypted.
- **Training and Compliance** – Develop a comprehensive privacy training program for all staff at the time of hire combined with annual refresher training. An internal communications campaign should also be taken to provide constant reminders of privacy protocols and practices.
- **Accountability** – Appoint a Chief Privacy Officer with overall responsibility and accountability for privacy and to establish the Technology Services department as a centre for responsibility for the delivery of training and support to staff as well as implementation of reasonable measures to protect personal information.

The Commissioner has also recommended that the Government of Ontario ask the Auditor General to conduct privacy audits of the information management practices of selected public sector agencies. In addition, she has asked the government to conduct a review of the *Election Act* to ensure that the privacy and security of personal information in the custody and control of Elections Ontario, is strongly protected and is used prudently, as prescribed.

About the Information and Privacy Commissioner

The Information and Privacy Commissioner is appointed by and reports to the Ontario Legislative Assembly, and is independent of the government of the day. The Commissioner's mandate includes overseeing the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*, as well as the *Personal Health Information Protection Act*, which applies to both public and private sector health information custodians. A vital component of the Commissioner's mandate is to help educate the public about access and privacy issues.

Media Contact

Rob McMahon
Director of Communications
Office: (416) 326-3902
Mobile: (416) 627-0307
media@ipc.on.ca