OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

BY FAX

March 24, 2006

Dave Nikolejsin, Chief Information Officer
Ministry of Labour & Citizens' Services
4000 Seymour Place
Victoria, BC V8X 4S8

Dear Dave Nikolejsin:

Ministry of Labour and Citizens' Services—provincial government computer system security—OIPC File No. F06-28107

I enclose for your information a copy of my letter of even date to Mike Farnworth MLA, responding to his March 7, 2006 letter asking me to investigate a "probable breach of the security system protecting the Provincial Government wide computer network" between December 2005 and February 2006.

In the course of our inquiries, we learned that the provincial government does not have any rules in place preventing personal information from being stored on desktop computers connected to the network, as opposed to being stored on secure servers. This is something that the provincial government should move to address, my view being that computer files containing sensitive personal information should not—except in the rarest cases and even then only if encrypted—be stored on networked desktop computers or on laptops (in the latter case, whether connected or not). I am aware that a similar recommendation—recommendation 7—is found in the report issued today regarding the government's investigation of the sale of computer backup tapes containing personal information.

A copy of this letter and my letter to Mike Farnworth MLA has been sent to the Hon. Mike De Jong because the matter was raised in the House.

Yours sincerely,

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

cc: Hon. Mike De Jong, Minister of Labour & Citizens' Services

Gordon Macatee, Deputy Minister, Ministry of Labour & Citizens' Service

Enclosure (1)

F06-28107 Nikolejsin Letter (Mar 24 06).doc

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

BY FAX

March 24, 2006

Mike Farnworth MLA
Opposition House Leader
Parliament Buildings
Victoria BC V8V 1X4

Dear Mike Farnworth:

Ministry of Labour and Citizens' Services—provincial government computer system security—OIPC File No. F06-28107

This letter responds to your March 7 request that I investigate a "probable breach of the security system protecting the Provincial Government wide computer network" between December 2005 and February 2006.

In my March 7 response to your request, I noted that the *Freedom of Information and Protection of Privacy Act* ("FIPPA") does not impose information security obligations in relation to general, non-personal, information in the custody or control of public bodies. Section 30 of FIPPA requires public bodies to make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information. In this light, I indicated that part of my inquiries would involve determining whether personal information of any individuals was involved in any incident that may or may not have occurred.

My office has carried out inquiries with the Information Security Branch ("ISB") of the Office of the Chief Information Officer. The ISB is responsible for investigating computer security matters for the provincial government. Our inquiries involved a review of the investigation reports produced by the ISB and discussions with ISB staff. Because the incidents had been investigated before we became involved, we have relied on information provided to us by the ISB, whose representatives co-operated fully with our requests for information and documentation.

Our inquiries disclosed that there were three separate ISB investigations in January and February of 2006. In each case, suspicious activity was noted on one or more provincial government computer systems. The ISB removed the computers involved from the government system and analyzed a sample of the computers. In each case, the computers were compromised by remote access

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Third Floor, 756 Fort Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through *Enquiry BC* at (800) 663-7867 or (604) 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

software and were being used for peer-to-peer file sharing. The computers were then securely erased and returned to use.

ISB staff told us that, because they had identified situations of this kind as recurring, a system-wide scan of similar suspicious activity was carried out in February, 2006. This scan identified approximately 90 workstations that displayed behaviour indicating they might have the same malicious software present. Further analysis reduced this number to 78. In order to ensure that all possibly affected machines were dealt with, a broad cleanup approach was approved. No further analysis was done on the 78 computers and they were all securely erased before being returned to use. This cleanup happened during February and March of 2006.

The ISB's investigation indicated that the incident involved unauthorized third-party use of computer workstations for peer-to-peer sharing of files placed on the workstations by third parties. It appears that hackers had exploited vulnerabilities in software on the affected computers, since security patches for these vulnerabilities had not deployed as expected. The ISB found no evidence of any attempts to access other computer resources such as databases or servers. The ISB also did not find any evidence that those involved had used usernames or passwords to attack the workstations.

It is not possible at this stage for me to determine with absolute certainty whether these incidents in any way exposed anyone's personal information to risks such as unauthorized access, collection, use, disclosure or disposal. Based on our inquiries, however, it is reasonable to conclude that third parties exploited security vulnerabilities solely to commandeer computer workstations and use them for peer-to-peer file sharing by third parties. Accordingly, in the absence of better evidence suggesting exposure of personal information to risks such as unauthorized access, collection, use, disclosure or disposal, I am not prepared to open a full investigation into this matter on the basis of the facts known to my office at this time.

Section 30 of FIPPA requires provincial government ministries and other public bodies to ensure that personal information is protected by reasonable security measures. This is not a standard of perfection, and there will always be some degree of risk, since no computer system connected to the internet is immune to attack and exploitation. Nonetheless, s. 30 requires public bodies to take reasonable measures to protect against attacks and to deal with them expeditiously and effectively when they are discovered.

Information security measures are properly established through a methodical assessment of risk that assesses both the foreseeability of a privacy breach (intentional or accidental) occurring in the context of current threats to or weaknesses in existing information-security measures and the severity and extent of the foreseeable harm that could result from a privacy breach. This assessment should then be used to identify and implement a hierarchy of security measures according to the degree of risk involved.

Because information security threats are constantly and rapidly evolving, the assessment of risk and implementation of steps to protect against risk must be undertaken regularly and on an ongoing basis. Organizations in both sectors must be vigilant and pro-active in the assessment of information security risks and measures.

In the course of our inquiries, we learned that the provincial government does not have any rules in place preventing personal information from being stored on desktop computers connected to the network, as opposed to being stored on secure servers. This is something that the provincial government should move to address, my view being that computer files containing sensitive personal information should not—except in the rarest cases and even then only if encrypted—be stored on networked desktop computers or on laptops (in the latter case, whether connected or not). I am aware that a similar recommendation—recommendation 7—is found in the report issued today regarding the government's investigation of the sale of computer backup tapes containing personal information.

I will have more to say about general principles of personal information security in my forthcoming report on our investigation into the sale of provincial government computer backup tapes containing personal information. Since analysis of the tapes involved in that situation continues, my report is not likely to be ready for release until some time next week.

A copy of this letter has been sent to the Hon. Mike De Jong because the matter was raised in the House.

Allow me to thank you for asking me to look into this matter.

Yours sincerely,

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

cc: Hon. Mike De Jong, Minister of Labour & Citizens' Services

Dave Nikolejsin, Chief Information Officer
Ministry of Labour & Citizens' Services

Gordon Macatee, Deputy Minister
Ministry of Labour & Citizens' Service