Investigation Report

2006-048 – Loss of custody of 41 computer data tapes containing personal and sensitive information

Introduction/Purpose of Report

On March 3, 2006 the Chief Information Officer, (CIO) for the Province of British Columbia was notified that the Vancouver Sun newspaper was investigating the sale of provincial government computer tapes containing personal and sensitive information. This report focuses on the government's investigation of the incident (including the scope, methodology and findings).

The report will also include specific findings, conclusions and recommendations that are intended to address areas requiring improvement identified to date (i.e., policies, procedures and processes).

Although the investigation is ongoing and may result in additional findings and recommendations, sufficient progress has been made to report, with a strong degree of confidence, on:

- The actions and activities of Ministries and individuals that resulted in the disclosure of sensitive personal information on 41 computer data tapes acquired by the Vancouver Sun newspaper;
- Who had access to the tapes from the time they left government's custody and control until they were recovered by government;
- The results of the review of policies and procedures as they relate to data storage devices and specifically computer tape disposal practices; and,
- The extent and type of information placed at risk.

Recommendations regarding disciplinary action are not within the scope of this investigation.

Assumptions

- While the veracity and "good faith" of all parties were assumed, unless evidence indicated otherwise, other scenarios were considered including criminal, malicious or nuisance intent.
- The Provincial Government would honour the purchaser's desire to remain anonymous[1].

[1] The Province has undertaken that it "will not attempt to learn the identity of the individual who purchased the 41 tapes". This was a condition of the purchaser agreeing to swear the affidavit in Appendix B. The agreement was facilitated directly with the purchaser by the Office of the Information and Privacy Commissioner.

- The investigation would include the sale of Blackberry hand-held device(s)[2] only as it relates to this specific incident under investigation.
- No further sales of provincial government surplus storage media would be conducted during the course of the investigation[3].
- All resources necessary to conduct the investigation would be made available.
- There would be full and transparent cooperation with the Office of the Information and Privacy Commissioner of British Columbia and his investigative team, including Forensic Data Recovery (FDR[4]).

Methodology

On March 3, 2006 the Minister of Labour and Citizens' Services directed his deputy minister to lead the corporate effort to manage the response to this incident, including conducting an investigation on behalf of government. The deputy minister designated the CIO to coordinate efforts across government in support of the Minister's direction.

On March 4, 2006 the Information Security Branch of the Office of the CIO was requested to undertake an investigation and a lead investigator was assigned.

A team composed of individuals with the expertise and knowledge required to conduct a thorough investigation was formed. The team met daily throughout the investigation. Team members were representatives of the Office of the CIO, responsible for privacy and security, legislation, policies and standards; Common Information Technology Services, responsible for computer assets; Asset Investment Recovery (AIR), responsible for asset disposal; and, ministry representatives from ministries of Employment and Income Assistance (MEIA) and Children and Family Development (MCFD), responsible for management of information within their custody.

The Office of the Information and Privacy Commissioner, responsible for independently monitoring and enforcing the B.C. government's privacy legislation, was invited to participate as an observer for all aspects of government's investigation.

Immediate attention was focused on government gaining possession of the tapes; this was essential for both investigative and privacy reasons.

While the tapes were being acquired an investigation plan was created that met the needs of both the Office of the Information and Privacy Commissioner and the Office of the CIO.

The team identified and reviewed all applicable government records including sales records, documented procedures, digital photos, asset disposal forms, etc. Interviews

[2] See Appendix A
[3] The Honourable Michael de Jong, Minister of Labour and Citizens' Services made this permanent on March 7, 2006.
[4] Forensic Data Recovery is a company that specializes in the forensic recovery and analysis of data on computer and computer storage devices. FDR is working under contracts from both the Province and the Privacy Commissioner in conjunction with this investigation.

were held with key personnel to verify records and provide additional information regarding who had custody of the tapes at each point during the disposal process. The team reviewed legislation, policies and procedures currently in place to determine if a gap contributed to the breach.

Chronology

Friday, March 3, 2006
The Office of the Information and Privacy Commissioner received a call from a reporter at the Vancouver Sun newspaper who indicated that he was investigating a story regarding the B.C. government's sale of computer tapes containing sensitive and personal information. The Office of the Information and Privacy Commissioner contacted the CIO. The CIO arranged an emergency meeting with senior government officials to focus on how to safeguard the information and retrieve the tapes. A decision was made to stop sales of all tapes or storage media.

Saturday, March 4, 2006
A formal investigation (2006-048) was launched. A lead investigator and forensic analyst from the Office of the CIO were assigned. Work began to retrieve the 41 tapes and determine how they ended up in the possession of the Vancouver Sun newspaper.

The article run by the Vancouver Sun titled[5] "Health Records Sold at Public Auction" indicated that the computer tapes had been sold for approximately three hundred dollars. A close up photograph included in the article showed one of the tapes clearly labelled VAN590W8TH. It was determined that MEIA had closed an office at 590 West 8th Avenue, Vancouver in July 2005.

It was determined that MEIA would act as the ministry of primary responsibility as it appeared the bulk of information related to their current ministry. MCFD continued to participate in the investigation team meetings to ensure historical linkages between the organizations and the information were addressed.

Gathering of records from Asset Investment Recovery began and included general data covering sales of tapes/tape drives for the past two years, as well as specific data that might indicate that the tapes had been sold through AIR. A specific form for disposal of goods located at 590 West 8th Avenue was identified. This form was date stamped March 14, 2005.

The Vancouver Sun informed the Office of the Information and Privacy Commissioner that the 41 tapes were in secure storage and the newspaper did not intend to access the tapes further.

Government's legal counsel prepared a formal affidavit for the Vancouver Sun and the purchaser to sign attesting that information from the tapes had not been saved, copied, or

[5] See Appendix A

shared with other parties and that all copies were returned to government. The Office of the Information and Privacy Commissioner offered to facilitate neutral communication of the affidavits to the purchaser and the Vancouver Sun and the physical retrieval of the tapes.

It was clarified that the stop order on computer sales and related media applied to all computers, including those coming from the federal government and other sources sold through AIR.

Sunday, March 5, 2006
Work continued on arrangements for retrieval of the tapes.

Monday, March 6, 2006
The Vancouver Sun published an article titled "Refugee Claim Files Found on Data Tapes". This article reported the data tapes were "sold for $101 at a B.C. government auction house".

Further clarification of the stop order was made. The stop order included the sales of all technology items. This included but was not limited to computers and peripherals, salvage pieces, monitors, digital cameras with removable drives, printers, monitors, keyboards, mice, servers, back up UPS units, wireless equipment, photocopiers, fax machines, portable USB drives, smart cards, and data tapes. AIR was advised of this directive.

FDR took possession of the 41 computer tapes from the Vancouver Sun and placed these in secure storage.

The purchaser signed an affidavit[6] that he or she had not used the personal information and had not made copies of the tapes on the condition that the Province would not attempt to learn the identity of the individual who purchased the 41 tapes.

The purchaser was reimbursed for the full amount paid for the tapes plus a small amount to cover minor incidental expenses incurred in dealing with this incident.

The Vancouver Sun reported it had copied information from some of the tapes onto one DVD and three CDs. The Vancouver Sun remains in possession of these copies. The Office of the Information and Privacy Commissioner communicated with the Vancouver Sun concerning the content and security of the DVD and CDs and the purpose for continued retention. The Vancouver Sun reported that it had deleted all information copied off the tapes from its servers and further agreed to conduct a second, more thorough deletion process.

[6] See Appendix B

Tuesday, March 7, 2006
The Vancouver Sun and the Victoria Times Colonist published further articles "Welfare worker had escort licence, stole rent cheques" about the data on the tapes.

AIR identified that there was one lot of federal assets (# 54) sold in May 2005 that matched the dollar value ($101.00) reported by the Vancouver Sun. A photograph of the lot was provided to the investigation team. The photograph showed a pallet with a number of tape drive units and two closed cardboard boxes. The contents of the cardboard boxes were not itemized.

The Honourable Michael de Jong. Minister of Labour and Citizens' Services made the ban on the sale of all data storage media permanent on March 7, 2006.

Wednesday, March 8, 2006
The Vancouver Sun published an article "Privacy Nightmare – Personal Data Sold with Blackberrys"[7] stating that the B.C. government sold Blackberrys, handheld wireless communications devices, that contained personal data. A parallel investigation into this incident was started. Government began attempts to gain possession of the Blackberrys and to ensure the protection of any personal or sensitive information. As part of this effort, invoices for Blackberrys sold during the time period of interest were pulled from the AIR systems. The invoice for the specific sale was identified and a query was run for all purchases made by the same purchaser, to determine if there was a potential for additional exposure. This cross reference revealed that the same person who purchased the Blackberrys also purchased lot 54 suspected of including the 41 tapes. Consequently, the investigators were in possession of the identity of the purchaser of the 41 tapes so additional measures were put in place to maintain the confidentiality of this information, including sealing of the original transaction record for lot 54.

An additional investigation was conducted to determine if these incidents were coincidental or targeted acts by an individual acting alone or in collusion. It was determined that the purchaser had never been a B.C. government employee nor were any records discovered that indicated any previous significant dealings with government. A check was also performed to determine if any of the AIR employees had been previously employed by MEIA or had any documented relationship with the purchaser. No such evidence was found.

The sale price for lot 54 and the Blackberrys totalled three hundred dollars which matched figures quoted in the original Vancouver Sun articles.

Twenty-one of the tapes were physically marked as originating from 590 West 8th Avenue. The origin of the other 20 tapes could not be determined through a physical examination.

[7] See Appendix A

Forensic copies of the tapes were made in order to allow investigators to review the data contained on the tapes while maintaining the integrity of the original tapes (a process that took several days).

The lead investigator met with the Director of Asset Management and Product Supply who is responsible for AIR staff. Information was gathered relating to the processes and common practices in use at the location. The bills of sale and photographs of all relevant lots were reviewed.

The interviewee indicated the following:

- AIR receives assets to be disposed of from the B.C. government, the broader public sector and the federal government;
- The money raised from the sale of the assets is returned to the original owner;
- Assets are pulled together to make an attractive sale lot; and
- Assets from the B.C. government, the broader public sector and the federal government are not normally mixed together to make one lot because it would be too difficult to divide the proceeds of the sale.

Friday, March 10, 2006

Analysis of two of the tapes was completed. Both tapes contained large volumes of data. Work continued on the rest of the tapes. Additional computer equipment was brought in to speed up the restoration process.

Interviews were held with four Ministry of Employment and Income Assistance staff who were directly involved with the move out of 590 West 8th Avenue. A timeline for the ministry office move was established as a result of these interviews. In January of 2005 the former Ministry of Human Resources began preparations to vacate their offices at 590 West 8th Ave. in Vancouver. At its peak the Ministry occupied the entire building, but after 2004 occupied two floors of the building with approximately 100 staff located on site.

The interviewees indicated the following:

- Move activities included identifying what computer components would be reused, which would be used as parts and which components would be disposed of. These components were servers, keyboards, monitors, tape drives and backup storage tapes;
- Approximately four individuals were involved in the exercise to dismantle the existing computer rooms in preparation for the move;
- Specific individuals within the ministry were tasked with the responsibility for ensuring all computers were wiped of all personal information per government policy and that all backup tape media were destroyed;
- Assets that were sent to Asset Investment Recovery for disposal were accompanied by the proper paperwork (Sample blank form attached – Appendix D);
- The disposal forms were not signed off by the appropriate Ministry management (there was no management level signature included). Disposal forms were signed

off by the Team Lead (non management personnel) and a contracted resource attesting to the fact that all the equipment had been properly "wiped" of personal information before leaving the Ministry;
- No one interviewed remembered sending a box with tapes to Asset Investment Recovery;
- MEIA staff responsible for handling the tapes indicated they were aware of ministry procedures requiring the destruction of tape media and all believed that this was always done. A review of ministry documentation supported that the ministry disposed of tapes through destruction on three occasions in 2005;
- It was indicated because of the volume, individual tapes were never inventoried. There is no exact count of how many tapes were in use;
- Everyone interviewed expressed the opinion that there was loose unattended material, boxes and supplies throughout building due to the impending office move; and,
- The boxes containing the tapes and the computer equipment designated for disposal were stored in the same secure room. One interviewee suggested that it was possible that boxes got mixed during the move process.

Progress continued on the tape copy process. Twenty-one of the 41 tapes had been forensically copied. Determination of the status of 18 of the tapes was still underway. Two tapes had yet to be copied.

A high level plan was created to allow analysts to classify the data on the tapes during the analysis phase.

Monday, March 13, 2006

The Office of the Information and Privacy Commissioner was satisfied with the Vancouver Sun's proposed plan for securing the DVD and CDs on which it had continued to retain personal information from the 41 tapes and ensuring that the DVD and CDs would not be exposed to risk of unauthorized access, pending any further clarification and confirmation of their content and status.

A preliminary analysis report was provided to the investigation team. The report[8] provided a brief summary of the findings to date of the analysis of the data on the tapes. The files were analyzed for data containing the following types of information:

Personal Information:
- Name (surname and first name)
- Date of birth or age
- Child and Youth information

Unique Identifiers:
- Social Insurance Number

[8] Preliminary Findings of the Forensic Data Analysis of Recovered DLT Tapes. Report provided by Forensic Data Recovery Inc.

- Driver's license number
- Medical Services Plan number
- Other identifiers (GAIN, Immigration, etc.)

Specific Descriptions or Attributes:

- Medical
- Employment
- Financial
- Immigration
- Solicitor / Client
- Other

Tuesday, March 14, 2006

A table listing the findings by tape is included in Appendix C. A single tape with a last usage date of July 2005 was discovered to contain a backup of the purchaser's personal computer system.

Findings

Policy Review

The *Freedom of Information and Protection of Privacy Act* (FOIPP Act) and the *Document Disposal Act* (DDA) relate to this investigation. The FOIPPA specifically assigns responsibilities to public bodies (ministries, provincial agencies, and other government bodies) for the collection, use, disclosure and disposition (including destruction) of personal information. Section 30 of the FOIPP Act states: "A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

The DDA states that no government records can be disposed of without specific legislative authority (i.e., approved records/schedules).

The Core Policies and Procedures Manual (CPPM), Chapter 12, provides corporate policy regarding information and information technology management and Chapter 12 supplementals provide policies and procedures for the FOIPP Act and the DDA. Chapter 12 specifically states that: "Ministries are responsible for ensuring that the electronic storage, retention and disposition of data are consistent with government records management policies, in accordance with the *Document Disposal Act* and *The Freedom of Information and Protection of Privacy Act.*"

Chapter 12, Information Technology Security Policy (ITSP), requires that: "Erasable media must not be released for reuse, destruction, or resale until it has been sanitized using an approved government erasure procedure. Ministries must be able to implement proper data destruction methods for confidential or highly-sensitive material, rather than relying on third parties."

Recorded information management destruction policies require that records be destroyed:

> "Using methods appropriate to their medium to ensure complete obliteration of the information (i.e. microfilm, microfiche, magnetic computer tapes, compact disks and diskettes must be destroyed in a manner that ensures the information contained in the media cannot be reconstructed). Shredding and then incinerating the materials is considered the most effective method of destroying microforms, magnetic tapes and compact disks and diskettes."

For the disposition of government records, ministries are required to "develop internal procedures and approvals for disposition and that the confidential destruction of records, including any existing backup, duplicate and/or security copies, is fully documented". MEIA did have local operating procedures that addressed the destruction of data storage tapes.

Chapter 15 of the CPPM deals with security from the risk management perspective, and specifically provides that:

> "Each ministry must protect information holdings in all physical, electronic and digital formats commensurate with its value and sensitivity at all stages in the life cycle of the activity to preserve the confidentiality, integrity, availability, intended use and value of all records. Security categories approved by Risk Management Branch must be used."
>
> "Ministries must identify and categorize information and other assets based on the degree of injury (low, medium, high) that could reasonably be expected to result from compromise to their availability or integrity, with reference to the provisions of the *Freedom of Information and Protection of Privacy Act* or other legislation."

Contrary to the above, during the course of this investigation there was no indication either documented or verbally communicated that any of the electronic information in question had an information classification assigned to it.

Existing Accountability Framework

The above noted legislation and core operating policy and procedures clearly assign accountability at the ministry level for the collection, management and disposal of confidential personal information. The deputy minister, as the senior public servant within each ministry, has ultimate accountability for ensuring that their ministry is in compliance with all aspects of legislative requirements and the CPPM.

Within each ministry there are designated positions to deal with day-to-day management and compliance (including education/training) with the various aspects of the CPPM. For example, Directors/Managers of Information and Privacy (DMIP's) are responsible for administering all ministry accountabilities under the FOIPP Act and core policy.

Ministry Records Officers (MRO's) are responsible for administering the ministries' records management requirements under the DDA and CPPM. Ministry Data Administrators are responsible for data management and data standards.

Ministries also typically have additional positions such as ministry level Chief Information Officers and Information Security Officers, but those positions and the specific accountabilities assigned to them vary from ministry to ministry.

These positions commonly use specific and detailed forms to ensure accountable positions certify procedures have been correctly followed. For example the "Disposal of Computers" form used by AIR requires dual sign-off that assets have been properly wiped of personal or sensitive information.

Ministry of Employment and Income Assistance

Upon hearing about this incident the ministry's first concern was the recovery of the information and finding out how a disclosure like this could have happened. MEIA initiated processes to deal with any contacts from concerned citizens/clients and continues to maintain this commitment.

MEIA had procedures in place that expressly prohibited the sale of computer data tapes. Staff were aware of and trained in these procedures as is demonstrated by the documented destruction of tapes throughout 2005.

Inventorying of tapes was not conducted as it was considered too labour intensive due to the number of tapes in use.

Most tapes were not labelled and those that were only indicated the street address of the office. There was no indication of the type or classification of the information resident on the tapes.

Tapes were not encrypted, however, at the time the tapes were generated (1998-2001) this would not have been common practice outside of high security installations.

Staff were aware of government asset disposal processes but did not fully understand their specific responsibilities as related to the FOIPP Act. The "Disposal of Computers" form includes a quoted reference[9]. It is unclear what is being quoted. It was clear that staff believed requirements to "wipe" equipment indicated on the form was limited to hard drives. No consideration was given to other data storage types.

Ministry staff did not complete documentation at a sufficient level of detail. This resulted in an incomplete listing of the specific assets that were sent for either disposal or destruction. Combined with a lack of inventory, this resulted in the inability to make

[9] "It is the responsibility of each Ministry to ensure all computers are erased of all information prior to Asset Disposal, Transfer or Re-Use by Schools, Charity Groups".

conclusive findings in several areas including the number of tapes that were disposed of through AIR.

Computer equipment to be shipped for asset disposal was stored in the secure server room along with boxes of tapes to be destroyed. Both the computer equipment and the tapes were packed into similar looking cardboard boxes. It was determined that it was possible that a box of tapes was sent accidentally with the computer equipment to asset disposal.

Specific positions that were directly involved with and responsible for the move of the facilities and the disposition of the storage media have been identified. The Manager, Operations was responsible for the procedures in place at the time and for their enforcement.

The possibility that the release of the confidential tapes was a deliberate act was explored; however, there was no evidence to support this.

Asset Investment Recovery

Asset Investment Recovery (AIR) is a branch within the Common Business Services Division of Labour and Citizens' Services. The AIR warehouse in Surrey where the tapes were sold employs approximately ten staff, one of whom is in a supervisory position.

AIR receives physical assets for disposal from many different public sector organizations. The federal government, municipalities, and crown corporations all make use of AIR's disposal services, including the disposal of used computers and computer related equipment. In all cases and for all customers AIR relies upon the originating entities local policies and procedures to ensure that any assets transferred to AIR for disposal have been certified to be free of any confidential information.

AIR's "Disposal of Computers" form[10] clearly states the requirements for the "wiping" of data from hard drives is a ministry responsibility. Specific reference to the requirements under the FOIPP Act is included. With regards to this incident under investigation the AIR staff did receive a signed "Disposal of Computers" form. An issue that the investigation team discovered is that the average person completing this form may not understand the breadth of the ministry's requirement to "ensure all computers are erased of all information." The form specifically references hard drives twice while there is no reference to any other data storage types. Also, the form does not indicate sign-off must be performed by government personnel and approval of disposal must be authorized by a government manager.

Notwithstanding the originating ministry accountability to certify that computer assets are free of confidential information, AIR staff do perform additional checks wherever possible to ensure protection of confidential information. It is the local operating policy

[10] Attached as Appendix D

of the AIR branch that, if discovered, data tapes and other removable media, originating from provincial ministries, are destroyed.

Staff indicated they were aware of government asset disposal processes and believed that not only were they acting in compliance with those processes, but they also developed additional local procedures, for added assurance, on their own departmental initiative. It was clear the staff believed requirements to "wipe" equipment indicated on the "Disposal of Computers" form was limited to hard drives.

When assets from the provincial government, the federal government or the broader public sector are received at the Surrey Asset Investment Recovery site staff keep the assets separate. Provincial government assets are mixed and matched in order to make lots as attractive as possible to purchasers. Documentation exists to show that the tape drives sold to the purchaser originated within the federal government. Even though staff indicated they attempt to keep federal and provincial assets separate, it is reasonable to believe that the box of tapes originating with MEIA was added to lot 54. It was determined that it was possible that the tapes were received in a box with miscellaneous computer equipment and there was human error in not destroying the tapes.

Staff at the Surrey AIR do not remember receiving a box of 40 or more tapes. There was no inspection and no quality assurance process in place to guarantee that the tapes did not end up for sale.

All staff located at Surrey AIR were involved in the disposal process and may have been directly involved with the actions and activities that took place that resulted in the sale of the tapes. Management was responsible for the procedures in place at the time of the incident and for their enforcement.

General

Throughout the asset disposal process, from the time a ministry identifies an asset for disposal, to ultimate disposal by AIR, a number of general activities can be identified as follows:

- Identification of item(s) for disposal/destruction;
- Formal initiation of disposal/destruction;
- Management sign-off;
- Packaging of items;
- Transportation of items;
- Receipt of items;
- Creation of sale lots (disposal only); and,
- Final sale or destruction.

An individual was assigned responsibility for each activity. For all of these roles it was found that there was varying degree of general or specific training on government policy, procedures and processes. While all individuals interviewed indicated they were aware of government policy and their work group's procedures and processes it was evident that

the implementation was inadequate to meet policy requirements. Generally the following observation can be made:

- Existing forms, procedures and processes are inadequate;
- Insufficient level of detail to ensure checks and balances;
- No specific training or education supplied to responsible positions;
- No consistency in government procedures and processes;
- Inadequate documentation trail;
- Inadequate attention to existing policy and procedures.

In the area of packaging of items it was found there was no standard and no clear requirement for visible labelling that indicated the destination (disposal or destruction) and the detailed content types, including sensitivity.

Conclusion

It is clear that in order for government and the citizens of the province to realize the efficiencies and cost benefits that computerization can provide the public must have confidence and "trust" in the security and privacy of the information government holds.

The investigation confirmed that at a high level B.C.'s legislative and policy framework with respect to the management and destruction of data storage medium aligns well with those of other leading jurisdictions. Weaknesses appear to exist in how specific Ministries apply and execute these policies including their local operating procedures.

The investigation cannot give a definitive description of what occurred due to the lack of a tape inventory and inadequate documentation detail. However, the most probable conclusion is that the information provided by the purchaser of the tapes was accurate, i.e. government sold the tapes through a sealed bid offer to purchase process in May 2005. The sale occurred due to procedural and human errors. A lack of checks and balances within the system allowed these errors to compound resulting in the release of personal and sensitive information.

This investigation has concluded the most likely cause of the loss of custody of 41 tapes was an accident resulting from numerous procedural, process gaps and ultimately human errors. It has also confirmed the importance of rigorous government policies, practices and safeguards and has highlighted the need for regular "check ups", audits and response plans for dealing with incidents and issues as they are identified regarding governments' information holdings.

Even the best policies and practices are only as good as the knowledge, skills and diligence of the individuals who must administer them. Those in government who are charged with using and protecting personal information must have understandable policies and procedures to follow, they must be aware of those same policies and procedures and they must be trained and competent to administer them. This investigation demonstrates the required awareness and training are not fully in place.

The actions of individuals involved were not in compliance with existing policies and the level of awareness was inadequate in this situation. During the course of the investigation some other ministries were canvassed to discover their internal processes and it was found that similar deficiencies in the levels of awareness, education and compliance with policies and procedures are reflected elsewhere. This is an issue of concern that must be addressed.

Ongoing work continues to determine the extent and type of information placed at risk. However, it can be stated emphatically that a wide range of highly sensitive and personal information was placed at risk.

It is the opinion of the investigation team that there is no discernable risk to information at this time if government were to resume sales of electronic devices that do not contain storage media (e.g., monitors, keyboards, cases).

Recommendations/Decisions

The following recommendations are presented for consideration by government. While some of these recommendations may be addressed by policy and procedure work that is already underway, determination of this could not be done in the available time. While the ongoing investigation may result in some additional recommendations, sufficient progress has been made to determine that the following actions will not be contra-indicated. In considering the following recommendations government should take into account factors such as risk, security, confidentiality, privacy, cost effectiveness, and environmental impact.

These recommendations relate to all media that is capable of storing data including but not limited to: personal computers, laptops, personal data assistants (PDAs) such as Blackberrys, servers, multi-function devices, fax machines, data backup tapes and tape drives, storage discs, memory sticks, digital cameras, digital music devices, DVDs, CDs, and cell phones.

It is important to note that all of the following recommendations will only be as successful as the extent to which they are communicated, understood and applied diligently by all levels of the public service. Government will need to provide appropriate publication, education and training initiatives in order to meet this requirement.

Central Authority Accountability

1. **It is recommended that government undertake a review of corporate asset management policies, procedures, standards and practices.**

   The CIO, in collaboration with the Comptroller General, should review and amend asset management policies to improve tracking of the increasing array of information technology devices across government. This investigation has highlighted the need

for policy that considers not just the financial value of assets but the value of and risk to the information assets that may reside upon/within them (a $40 tape holding the personal information of thousands of British Columbians). Specific consideration should be given to the areas of compliance review and audit methods, procedural checks and balances, as well as education and training.

This review should also determine an appropriate method to implement an inventory management system for data storage media. This should include the classification of the information and the labelling and inventorying of the device.

2. **It is recommended that an external process for ensuring ministry compliance with information management policy be developed, including but not limited to, spot audits.**

3. **It is recommended that Government assign authority to the CIO to "shut down" asset disposal at any ministry identified as non-compliant with CPPM, or where, in the judgement of the CIO local procedures are insufficient to protect personal information from accidental release.**

4. **It is recommended that government continue the current ban on the sale of all media storage devices. Government should ensure that the list of what is banned is comprehensive, complete and regularly updated and is communicated to all necessary parties.**

5. **It is recommended that government consider the feasibility of encrypting government data on portable storage devices (e.g., Blackberrys, laptops, etc.) and on backup storage devices**.

6. **It is recommended that government update policy to include the reporting of lost portable storage devices, including storage media, (e.g., thumb drives, memory cards) regardless of financial value, within 24 hours from the time of loss.**

   This policy, in conjunction with new encryption practices, can mitigate the risk to government information in portable devices**.**

7. **It is recommended that government issue policy that all computer files containing personal information be stored on the government network and not on "non-encrypted" personal computing devices or data storage media (e.g., personal computer hard drives, laptops, PDAs, etc.).**

Ministry Accountability

8. **It is recommended that ministries conduct a comprehensive review of how ministry policies, procedures and processes for the disposal (including destruction) of computer assets are implemented in support of ministry accountability under the Core Policy and Procedures Manual**.

Additional training should be provided for all staff that have care or control of personal or sensitive information including disposal.

Ministries should designate a senior management position responsible for regular inspection and reporting regarding ministry compliance with all relevant legislation and policy related to the protection of personal or sensitive information.

Ministries should develop and communicate policy that explicitly states that managers who delegate responsibility for final sign-off on disposal or sale of any device or media covered under either the interim or the permanent ban are responsible for any actions taken by those to whom they delegate, including contractors or subordinates.

Ministries should conduct regular internal audits to ensure compliance with information management policy and must immediately address any deficiencies that are identified through either internal or external audits.

Specific documentation templates, procedures and accountabilities should be developed to ensure verification that no data storage media are included in any lots disposed by AIR. This includes non computer equipment lots.

9. **It is recommended that the management responsible at the two ministries involved in this incident (Ministry of Employment and Income Assistance and Ministry of Labour and Citizens' Services, Asset Investment Recovery Unit), identify the gaps in procedures and processes that resulted in non-compliance to policy. This will also include actions to immediately address these gaps.**

Personal Accountability

10. **It is recommended that government conduct a comprehensive review of current personal and management accountability mechanisms for all individuals involved in handling, labelling, storing or disposing of sensitive media or devices.**

    This should include the development and implementation of personnel policy that clearly outlines the individual accountability of all public servants who are required to handle, label or dispose of sensitive media or storage devices.