INVESTIGATION REPORT 2006 - 048

FINAL REPORT:

IMPLEMENTING THE RECOMMENDATIONS

Ministry of Labour and Citizens' Services
Office of the Chief Information Officer

August 2007

Table of Contents:

Introduction 1
Purpose of this Report 1
Implementation Methodology 1
Key Findings 2
1. Policy Review Findings 2
A. Central Agency (Core) Policy 2
B. Ministry Operational Policy 3
C. Personnel Policy 3
2. Accountability Findings 3
A. Central Authority Accountability - Recommendations 1 to 7 3
B. Ministry Accountability - Recommendations 8 & 9 10
C. Personal Accountability - Recommendation 10 13
3. General Findings 13
A. Information and Technology Governance Framework 13
B. Awareness and Training 14
C. Revised Security Policy 14
D. Resource Implications 15
Appendix A: Original Recommendations 16
1. Central Authority Accountability 16
2. Ministry Accountability 16
3. Personal Accountability 17
Appendix B: Office of the Information & Privacy Commissioner's Recommendations 18
How the recommendations were addressed in the OCIO activities: 18

Investigation Report 2006 - 048

Final Report - Implementing the Recommendations

Introduction

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. An investigation was undertaken by the staff in the Office of the CIO (OCIO). The Investigation Report 2006-048 - *Loss of Custody Of 41 Computer Data Tapes Containing Personal and Sensitive Information* (OCIO Report) was published on the CIO website on March 24, 2006. The report had 10 recommendations addressing accountability in three areas – central authority, ministry and personal.

The CIO established an Investigative Report Project Committee (the Committee) to address the 10 recommendations from the report (see Appendix A). This committee included staff from the Office of the CIO and Shared Services BC, which comprises Workplace Technology Services (formally Common Information Technology Services), and Common Business Services.

Purpose of this Report

Addressing the recommendations from the OCIO Report was intended to identify knowledge gaps in existing policy and to ensure implementation of proper information management practices and procedures. The focus in this report is to identify effective and efficient policy development, business process design, and risk management practices for all media with information storage capacity. This report summarizes the key results of the Committee's work on the recommendations from the OCIO Report.

Implementation Methodology

The Committee assigned a strategic lead for each recommendation to one or more executive staff from the three areas noted previously. The executive in turn assigned one or two senior management staff with implementation authority and responsibility. The management staff was responsible for developing work teams and resource/activity plans for each recommendation.

The project was assigned a project analyst whose functions included monitoring the work plan and developing a weekly report. The CIO submitted a weekly report to senior government executives. The CIO also corresponded with representatives from the Office of the Information and Privacy Commissioner during the implementation process to keep them apprised of progress. (Appendix B of this report addresses the concerns of Mr. David Loukidelis, Information and Privacy Commissioner for British Columbia raised in his investigation report F06-01; Sale of Provincial Government Computer Tapes Containing Personal Information.)

The Ministry of Employment and Income Assistance and the Ministry of Labour and Citizens' Services, Asset Investment Recovery Unit (AIR) assigned and developed work teams to work with the OCIO for recommendation 9. British Columbia Public Service Agency (PSA) staff worked with OCIO staff to address recommendation 10. A distinct team comprised of staff from the OCIO, ministries and a consultant was developed and assigned with the responsibility to review information and technology management governance within government.

The basic approach was for the working team to meet with identified stakeholders affected by each recommendation and complete the activities identified in the work plan that would address the recommendations. The end target date was set as June 30, 2006. Most Committee work plan activities for the recommendations were completed by this date. As a result of the Committee's implementation activities, operational business plan activities were identified that will be conducted over the longer term in specific areas e.g., encryption, information classification, and developing business processes related to implementing a new governance model.

Key Findings

Many of the OCIO Report recommendations required a review of policy, procedures and processes. Section 1 looks at the key findings in three policy areas, i.e., government core policy, individual ministry level policy and government wide personnel policy. Section 2 covers the 10 recommendations from the original OCIO Report and identifies key findings associated with the implementation of each of them. Section 3 looks at some general findings that are associated with addressing all of the recommendations. Factors such as risk management, security, information management, privacy, cost, and operational impact were considered during the implementation activities.

1. Policy Review Findings

A. Central Agency (Core) Policy

The Core Policy and Procedures Manual (CPPM) describes government-wide policy and establishes responsibility for policies of specific central agencies. The OCIO is one of these central agencies. The intended audience for the CPPM is all government managers and staff in general, and specifically any program manager, supervisor or other staff person with signing authority. Policies apply to all ministries, offices, special funds and accounts, and appropriations outlined in the Financial Administration Act. Policies also apply to the following officers of the Legislature: Auditor General, Police Complaint Commissioner, Information and Privacy Commissioner, Chief Electoral Officer, and Ombudsman. Crown corporations, public bodies and funded agencies are expected to follow the spirit and intent of policy requirements.

The OCIO Report referenced two major CPPM chapters. The first is Chapter 12, (Information Management and Information Technology Management) which, through delegated authority in CPPM Chapter 2, is the responsibility of the CIO. Chapter 15 (Security) is the responsibility of the Risk Management Branch (RMB) and is significantly related to information and technology security, which is the responsibility of the CIO through Chapter 12. Both were important in implementing the OCIO Report recommendations.

An OCIO CPPM policy review identified other chapters that deal with information and technology procurement (Chapter 6) and asset management (Chapter 8) mentioning responsibilities of other central agencies and Shared Services BC i.e., Office of the Comptroller

General (OCG), Common Business Services and Workplace Technology Services (WTS). In total there are nine core policy chapters that contain references to information and technology or are referenced from Chapter 12. There are also two CPPM procurement and asset management procedures that are relevant. Where required, these additional chapters and procedures were reviewed and used as part of the recommendations implementation.

B. Ministry Operational Policy

An overview of ministry operational policy related to disposal of assets capable of storing information showed that not all ministries are at the same stage of organizational maturity with documented local policies. Most ministries use a combination of standardized practice and policy, either local or central agency-based in managing asset disposal. This was addressed in recommendation 8.

C. Personnel Policy

CPPM notes that personnel policy is the responsibility of the BC Public Service Agency (PSA). Policy in CPPM chapter 12 does address appropriate use of information and technology, however, policy related to the terms of employment, standards of conduct or Oath of Office is the responsibility of PSA. As noted earlier PSA staff worked with the OCIO to address recommendation 10.

2. Accountability Findings

A. Central Authority Accountability - Recommendations 1 to 7

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

Status - Complete with ongoing OCIO and Shared Services activities

A work team report was submitted to the CIO with recommendations for ongoing business plan activities that are assigned within the OCIO. Over time these will strengthen the following:

a) Core policy clarity, awareness and use,
b) Compliance reviews,
c) Education and training,
d) Inventory management,
e) Safeguarding personal information, and
f) Information technology procurement and asset management/disposal.

In June 2006 changes were made to CPPM Chapters 8 (8.2 and 8.3) and 6 (6.3.4 d) through cooperation of the OCIO, RMB and the OCG. The Comptroller General approved and posted these changes in June 2006 and informed the ministries.

- Section 8.2 was revised to clarify that government assets include tangible capital assets and property, inventory, financial assets and other non-capital items including portable device technologies with information capacity and the information that is held on such devices/media.
- Section 8.3 was revised to emphasize the internal controls for protecting information that is stored on a portable device/medium, disposing of storage assets with information

capacity, and safeguarding of information as an asset irrespective of the physical asset's financial value.

- Sub-section 6.3.4 (d) was revised to add that the disposal of an asset/medium with information storage capacity must be done in a manner to protect the privacy and security of information.

An Information Security Classification Schema project was conducted as part of the Security Enhancement Project with leadership from the OCIO and the RMB. The proposed classification schema was reviewed and approved by the CIO and the Executive Director of the RMB. This approval allowed work to begin on a Risk Assessment and Impact Analysis to determine the scope and complexity of implementing an Information Security Classification Schema. This work is currently still underway.

A review of current central agency asset disposal processes was done by the OCIO. It found that, under government procurement policy (i.e., CPPM Section 6), there are two sets of services and processes available for the destruction of ministry records and IT equipment/media:

- The two Corporate Supply Arrangements for onsite and offsite records destruction administered by the OCIO Corporate Information Management Branch; and
- An asset disposal services administered by AIR for destruction of IT equipment and media (via Rider/Genesis and Budget Steel).

It also found WTS could further arrange for the destruction of client workstations, backup media and server hard disks by means of the above processes in the following ways:

- Through the IBM contract, WTS Workstation Services arranges for the destruction of obsolete client workstations and related peripherals using the AIR destruction processes.
- Workplace Hosting Services arranges for the destruction of client media (e.g., backup tapes) via the Corporate Supply Arrangement for offsite records destruction, and arranges for the destruction of server hard drives via AIR.

Shared Services BC performed an operational review of their information and technology asset management procedures, standards and practices that support the CPPM policies. The review involved policies from seven CPPM chapters and was designed to look at the corporate information technology asset lifecycle. The findings showed that corporate assets are managed according to policy. However, documentation regarding procedures and compliance requires improvement. Six recommendations to improve corporate asset management policies, procedures, standards and practices were identified:

- Increase awareness and training on policies and procedures;
- Address gaps in policy related to commissioning and tracking assets;
- Review policies regarding assets under $1000;
- Identify and clarify accountability and responsibility for physical inventories;
- Develop means to articulate roles and responsibilities between Shared Services and ministries; and
- Collaborate with the OCIO in identifying and planning for impacts when policies change.

Operational planning is underway to address these recommendations arising from the review.

December 2006 Update: A Request For Proposal is being prepared to acquire a resource to perform a Risk Assessment on the new Information Security Classification schema. Completion date of the Assessment and Impact Analysis is dependant on resource availability. An awareness program for IT asset disposal security issues is being developed by Ministry of Employment and Income Assistance (MEIA) and the OCIO.

Existing Corporate Supply Arrangements and lease/rental contracts have been reviewed and renegotiated to include removal of electronic storage media prior to disposal. WTS is working with IBM contracted services to supply disposal services for all WTS-owned IT assets. Ministries are responsible for removal of electronic media storage devices on all Ministry-owned assets. The two destruction/recycling facilities (Budget Steel and Genesis Recycling) have had a review of their handling procedures and an onsite inspection of their security controls conducted by Information Security Branch. Budget Steel was found to have insufficient handling procedures and security controls and they are not approved for IT asset destruction. AIR has conducted research into providing a destruction capability at the Victoria warehouse location and is proceeding with business case justification. The Genesis facility in Aldergrove will be the primary destruction facility for IT assets until an alternate solution is available.

June 2007 STATUS: AIR (Asset Investment Recovery**)** has purchased and installed a shredder that will be used to dispose of small IT assets (i.e. BlackBerry, PDA, hard drives, thumb drives, CD/DVD and floppy drives). A pilot of the IT Asset Disposition process with the new shredder is to be completed by the end of June 2007.

Recommendation 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."*

Status - Complete with ongoing OCIO activities

June 2007 STATUS: The Compliance Unit has drafted an IT Asset Disposition Compliance Plan and has already put some areas of the plan into effect to deal with monthly validation in Asset Disposal Reports.

A spot audit approach was defined in a report to the CIO on recommendation 2. Initial site audits began October 2006. Spot audits are done onsite and used to validate that adequate controls are in place for secure and safe disposal of assets. A compliance assessment program will include standardized tools to assess compliance to security standards and best practices.

This approach employs the same audit criteria and asset disposal security control objectives discussed below in recommendation 3. Where significant issues arise from an audit, a shut down request will be made to the CIO until mitigation strategies can be implemented. A review schedule will be maintained to track and report on mitigation implementation strategies. An operational business plan was developed to review the approach with ministries and got endorsement from them in October 2006.

December 2006 Update: The audit process was reviewed with and endorsed by Ministry Information Management personnel. The Audit process was piloted with MEIA in early

December. WTS Workstation Support Services and the Service Contractor (IBM/Microserve) will be audited when their internal processes have been revised and documented, and they are ready to proceed with disposal of workstation equipment. All Ministries will be requested to provide a compliance audit by the end of February 2007.

June 2007 STATUS: On Jan 3, 2007 a memorandum from the GCIO was sent out to all ministries regarding IT Asset Disposal. The IT Asset Disposition process is operational and compliance checks are being done by reviewing the ADR (Asset Disposal Report) to actual assets received. All 19 ministries completed their Security HealthChecks by April 27, 2007. IBM has conducted a review of their internal disposal processes and has provided a document to OCIO for review. Asset management processes are being implemented to ensure adequate checks for removable media are completed prior to shipment from the client site.

Recommendation 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 judgment of the CIO local procedures are insufficient to protect personal information from accidental release."*

Status - Complete with ongoing OCIO activities

A draft approach was presented by the work team to the CIO to allow shutting down unsafe information and technology asset disposal practices. Compliance monitoring is an accountability and responsibility of the CIO as defined in the Core Policy and Procedure Manual Chapter 12.2.2 IM/IT Governance.

The central agency review from recommendation 1 was used to design a draft generic disposition process that was reviewed against those submitted from ministries through recommendations 8 and 9. This was used in designing a draft standardized government-wide disposition process. A draft business process model for review of potential issues and stopping unsafe disposal practices was developed and shared with ministries in relation to establishing a standard review process. The initial draft business process model included the use of draft screening criteria to measure individual disposition practices against. It identified possible disposal process review metrics and incorporated 46 control objectives from recommendation 8 with two additional ones on records management that form the basis for the spot audits. A series of consultations between the OCIO and ministries helped to arrive at a recommended approach.

December 2006 Update: The approach for determining unsafe IT disposal practices and issuing a stoppage order will be based on an onsite risk assessment by the Information Security Branch or an approved agent. The onsite assessor will attempt to have the Ministry immediately rectify situations where there is an immediate threat of information exposure and, if no support is received, will take steps to secure the situation. The stoppage order will be issued via a letter from the CIO to the Deputy Minister responsible for the area of concern.

A standard disposal process for information technology assets has been completed, communicated to Ministries, and implemented at Asset Investment Recovery. The process is accompanied by disposition and destruction standards associated with the

implementation of Recommendation 4 below. The disposal process has been tested with MEIA and WTS and proven effective at identifying inappropriate IT asset management situations while preventing accidental release of media storage devices. The process testing has illustrated the need to phase in the compliance checking with the Ministries while an awareness program is implemented.

June 2007 STATUS: The IT Asset Disposition Process security controls are working as indicated by no incident of sensitive information being released to the public since the disposal ban was lifted. If ministries do send sensitive electronic records, typically on flexible media, along with IT assets for disposal the parties involved are notified and an investigation is launched which includes completion of a risk assessment and action plan for addressing the situation. Any current issues are related to either a lack of awareness by Ministry staff in regional offices, or the accumulation of assets that occurred during the workstation refresh.

Recommendation 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."

Status- Complete with ongoing OCIO activities

In April 2006 a memo was sent out to all ministries that stated a permanent ban on sale of portable data storage media was in place. The list in September 2006 of allowable products for sale included; monitors, keyboards, mice, empty equipment cases, power supplies (i.e., adapters, batteries but does not include in UPS), network/printer cables, and docking stations/port replicators. A report was submitted to the CIO on this recommendation with four suggestions to improve security around asset disposal:

- Ministries can dispose only of OCIO approved assets,
- Each device must be inspected for electronic media storage capacity by a technically competent person prior to its final disposition,
- AIR Unit will host the approved asset disposal list on their website, and
- Information owners must display clear accountability around information management and for following documented policies, procedures and processes for asset disposal.

Changes that relate to the working team report included:

1. Any device that contains electronic records must be erased prior to any inter-/intra-ministry transfer including redeployment within the same ministry or via Asset Investment Recovery to another ministry.
2. No media storage devices should be disposed of through reassignment or sale to the public.
3. Ministries are responsible for destroying low cost removable media asset (CD, DVD, Tape, hard and floppy discs, etc.) as part of their records management process.

June 2007 STATUS: Any device that may contain records is to be securely transported to Asset Investment Recovery for final disposition.

The working team report also provided a risk scale for assets with recommended dispositions by category and a draft asset disposal disposition review form to be circulated to ministries for comment and acceptance.

December 2006 Update: An IT Asset Disposition website has been setup which contains all the final documents concerning the disposal process, the approved device disposition list, and a submission form for having new IT assets added to the disposition list. This site is accessible by all government employees and has been communicated to the Ministry disposal review participants and IM/IT Management. A team is in place to review the submissions and evaluate the risk of information exposure from selling the asset. A final report on the IT Asset Disposal Process implementation will accompany this report.

June 2007 STATUS: Compliance Program is looking at providing generic categories to the IT Asset Disposal List to replace the current list which is managed by make and model. The categories will be based on IT Asset type such as cellular phones, personal digital assistants, laptops, desktops, photocopiers, etc. and will include specific instructions for disposal (i.e. hard disks – all must be destroyed regardless of model).

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

Status - Complete with ongoing OCIO, WTS and Ministry activities

A summary briefing note and work team reports on the feasibility of encrypting portable and backup storage devices was submitted to the CIO and approved pending a formally distributed follow-on work plan The following tables show what devices were reviewed in the reports:

Table 1: Portable Storage Devices
Blackberries
Laptops
Memory Sticks and Other Portable Storage Media (e.g., disks, tape, personal devices, iPods/MP3 players)

Table 2: Backup Storage Devices
Tape – mobile
Tape – non-mobile
Disk – server attached
Disk – network attached devices
Disk – storage area network
Other devices (e.g., magnetic tape, optical disk jukeboxes)

Key considerations for a corporate approach to encryption include:

- Classifying data that requires encryption,
- Non-encryption protection alternatives or adjuncts,
- Costs to implement software and hardware encryption solutions,
- The ability to encrypt devices and manage encrypted data over time,
- Resource requirements to implement encryption and manage encrypted assets, and
- Resolving technical challenges for certain types of products, e.g., *BlackBerry*™ devices and storage environments, e.g., direct server connections.

For most devices, the encryption of information is feasible except for centrally managed servers. Major concerns that arose while determining the feasibility of encryption included implementation costs in the region of $100 Million, decreased processing speed and performance impacting business functions.

While the basic feasibility reports have been conducted considerable work is still required to develop the alternatives into recommendations for executive to implement encryption services. For example there is continuing work to:

- Limit distribution of unencrypted thumb drives until a safe encryption mechanism is implemented and a government standard identified;
- Encrypt all mainframe tape backups beginning July 31, 2006;
- Upgrade all *BlackBerry*™ software to version 4.0 to provide added security features.(Note: The manufacturer must also develop a production ready encryption service for information held on the *BlackBerry*™. The status of this work will be periodically reported by WTS to the CIO); and
- Use folder-based encryption methods to safeguard offline data folders on newly issued laptops until a government standard laptop encryption product can be identified and implemented.

December 2006 Update: As indicated above several technical issues have been encountered in attempting to implement encryption solutions. The majority of these are related to significant decreases in performance when encryption is enabled. While implementation of encryption on portable devices is feasible on a limited scale today, the government wide solution is a long term goal (2-5 years). An initial solution for document folders on managed laptops is available.

A project has been initiated by Security Strategies group within the Information Security Branch, OCIO to conduct research on encryption solutions. A project kick off meeting occurred January 16, 2007.

June 2007 STATUS: Encrypted thumb drives have been set as a standard and are now available to purchase through I-Store.

Recommendation 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."*

Status - Complete with ongoing Shared Services activities

The OCIO, OCG and the RMB work team developed revised CPPM policy wording related to reporting a loss of sensitive, confidential information or the loss of a portable device or a hand-held device containing such information (Chapter 8.3.3 and Chapter 15). Chapter 12 requires information and technology assets to be protected commensurate with the identified risks and security requirements and that information security incidents, events and weaknesses must be managed and communicated to the Government Chief Information Officer for corrective action, if appropriate.

In keeping with this approach the new CPPM 8.3.3 required a report must be made immediately upon discovering a loss of a portable medium with information capacity (e.g., a hard drive, thumb drive, memory card, magnetic or optical disks, etc.) containing sensitive, personal or confidential information or where there is an information or information technology related security incident. It further stated that for hand-held devices (e.g., Blackberries), the loss must also be immediately reported to the Shared Services BC Help Desk at 250 387-7000 so that the device can be disabled to prevent the loss, compromise or unauthorized disclosure of government information.

WTS developed a process and timelines for accommodating loss reporting and the remote wiping of government information from a *BlackBerry*™ hand held device through the Help-Desk.

December 2006 Update: Ministries have been made aware of the requirement to report device/information losses through an information session and via disposal process documentation. Further awareness will be accomplished through implementation of a government wide awareness program currently under development.

WTS has implemented a process for initiating the wiping of all records on a Government *BlackBerry*™ hand held device when the device is reported as lost.

June 2007 STATUS: Any media found via IT Asset Disposition process will be couriered to Investigations Unit, Information Security Branch, OCIO, Labour and Citizens' Services. The ministry responsible will be contacted and required to complete a GILR before the IT assets will be released to the ministry.

Recommendation 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.)."*

Status - Complete

A memo from the CIO was sent to all Assistant Deputy Ministers of Corporate Services regarding the appropriate use of portable devices and handling information. Key points in the memo included:

- Government employees and contractors are responsible for the information and storage devices under their care;
- Information on a portable device is intended for temporary use and must be transferred and stored on the government network as soon as possible; and
- Personal or sensitive information must be encrypted when stored on a portable device.

B. Ministry Accountability - Recommendations 8 & 9

Recommendation 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."*

Status - Complete with ongoing OCIO and Ministry activities

The OCIO developed a framework for ministry self-assessment of each organization's documented policies, procedures and processes related to asset disposal. The framework provided a breakdown of all central agency policies by four compliance categories: policy review, management accountability, training requirements, and controls and measurements. A template of 16 key questions was provided by the OCIO for ministries to conduct the review and organize input back to the CIO. An additional 46 security objectives on asset disposal were included as a guideline for ministries to use in addressing any gaps they found.

The security objectives are also discussed in the Key Findings section for recommendations 2 and 3. Ministries responded by submitting their findings to the CIO by the end of June 2006. Some ministries looked beyond asset disposal to consider asset management throughout the information and technology lifecycles and describing business flow diagrams.

An analysis of the ministry submissions was conducted to identify the levels of organizational maturity related to the policies, procedures and processes in place at the time of the Tapes Incident. In general ministries are aware of and use core policies as their primary guidance. Where ministries differ the most is in the documentation of operational ministry specific policies, procedures and processes. The analysis showed:

- Two-thirds of the ministries use incidence based auditing processes or standard business processes but did not have them documented. They used CPPM policy and CIO directives but without a documented interpretation of how to implement it within the ministry. Training was limited and there was no standard or routine review of personnel practices.
- The other one-third of the ministries used audits routinely, processes were documented, authorities were in job descriptions or by another written designation, routine staff evaluations were done, and local controls existed and were routinely used.
- Depending on the processes within each ministry and the degree of centralized or decentralized control, accountability for asset disposal rested in a variety of positions within ministry offices as well as field offices.
- All ministries identified changes they plan to implement over the next few months as funding and staff resources permit.

The OCIO worked with the ministries to prioritize and implement some standardized formats, processes and procedures that arose from the analysis of the recommendation 8 self assessments. Suggestions from ministries that were considered are:

- Developing a standard information and technology asset disposal procedure guide;
- Designing awareness and training material;
- Clarifying between financial and information and technology management policy regarding low cost technology assets;
- Developing an efficient inventory control system;
- Improving communications of new policy and directives; and
- Designing a tracking mechanism that includes verification of secure destruction.

Policy compliance by contracted and alternate service delivery providers was an area raised by some ministries, including the need for centrally developed standard compliance measures, control objectives, policy boilerplate information and accountability statements. The suggestion for standardized documentation is under consideration by the OCIO (see Appendix B).

December 2006 Update: A standard IT asset disposal procedure has been developed and incorporated into the Disposal Handbook. The procedure has been communicated to Ministries via presentations to IM/IT and Records Management staff. An awareness program is under development within MEIA and will be provided to all Ministries. WTS has been asked to provide IT Asset tracking. The disposal process implemented with AIR provides adequate IT asset tracking to ensure that devices sent to AIR for destruction can be tracked from the point of departure (typically a Ministry office) to the destruction facility, with confirmation of lot destruction. A project has been initiated by the Security Strategies group within the Information Security Branch, OCIO to develop a contract schedule (Schedule G) to address security requirements.

June 2007 STATUS: Security Strategies Unit is working on a Schedule G and it has been sent to our lawyers for review. Approval forecast to be in the fall of 2007.

Recommendation 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."*

Status - Complete

This recommendation is specific to the areas that were directly involved in the actual tapes incident. Both the Ministry of Labour and Citizens' Services AIR Unit and the Ministry of Employment and Income Assistance completed comprehensive reviews of their policies, procedures and processes. The ministries submitted reports to the CIO that were reviewed and accepted. In June 2006 letters were sent out from the CIO to the respective senior executives informing them of the requirement to complete their detailed work plan to address the gaps. The letters further informed the two areas that the OCIO will conduct periodic audits for CPPM compliance.

A spot audit was conducted by the OCIO of AIR's disposal facility in June 2006. The findings of this audit indicate the revised processes implemented after the initial AIR gap analysis will ensure safe and secure disposal of computer assets and media. Additional audit and inventory controls had been implemented to further reduce risk of inappropriate disclosure of information.

December 2006 Update: AIR continues to review and update procedures and processes to ensure the secure disposal of IT assets. This includes modification of existing facilities to ensure secure storage and segregation of duties. Inventory tracking procedures have been implemented on a temporary basis to ensure thorough identification of workstation and hard disk assets, and tracking of current location/disposition. Piloting of the procedures has resulted in the effective identification of inventory control issues within MEIA. It is apparent that several Ministries have insufficient resources to appropriately manage IT asset disposal, and have little or no inventory management capability for low cost IT assets. This will require a dedicated

effort by management to ensure compliance with asset management and disposal policies. As the owner and manager of the majority of IT assets across government, WTS should become the focal point for IT asset management.

June 2007 STATUS: The Compliance Unit of ISB has completed the review of all ministry Security HealthChecks and have updated the ministry CIO and Information Security Officers with the results and the ongoing plans of the Compliance Program.

C. Personal Accountability - Recommendation 10

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

Status - Complete with ongoing PSA activities

A working team of OCIO and PSA staff identified the activities needed to implement this recommendation. Subsequently a letter was sent from Lori Wanamaker, Deputy Minister, Labour and Citizens' Services to James Gorman, Deputy Minster BC PSA confirming that PSA would conduct key activities including:

a) Revising the Standards of Conduct as part of a modernization review of PSA policy strengthening the confidentiality section;
b) Sending a statement in template offer of employment letters, indicating that, as a condition of employment, employees are required to swear or affirm an Oath of Employment and comply with the Standards of Conduct;
c) Maintaining links in their orientation website to the Oath, Standards of Conduct and the Chapter 12 Appropriate Use Policy; and
d) Communicating changes when new policy is rolled out.

December 2006 Update: BCPSA is in the final stages of consultation with the BC Government Employees Union on the revised policy. Final signoff is expected in Q4 06/07. BCPSA has implemented a corporately available website containing an orientation section for new employees with links to information and documents on the Oath of Employment, Standards of Conduct and Chapter 12 appropriate use policy and the Internet Communications Technology Usage Agreement.

June 2007 STATUS: New orientation program for new employees has been developed and implemented.

3. General Findings

A. Information and Technology Governance Framework

An Information Management and Information Technology Governance Review Working Group (Governance Working Group) was established in April 2006 at the request of the Deputy Minister of Labour and Citizens' Services. The mandate of the Governance Working Group was to review and describe current accountability structures within government for information and technology management, assess the effectiveness of the accountability structures and identify any deficiencies and make recommendation for improvements. Framework reports were submitted to the CIO and the Deputy Minister in July 2006.

The framework contained 49 recommendations in the area of information and technology accountabilities. These accountabilities addressed four structural domains:

1. The position of the Government CIO,
2. The position of the ministry CIO,
3. Governing bodies, and
4. Legislative requirements.

The key focus of the review framework included:

- Formalizing relationships, responsibilities and lines of reporting;
- Integrating information and technology planning and services under the CIO roles; and
- Developing and making available corporate policies, procedures, business processes and standards.

The framework also identified the need to ensure the capability and sustainability of information and technology human resources at all levels.

B. Awareness and Training

Ministries must take operational responsibility for appropriate awareness and training initiatives and for ongoing supervision regarding personal accountability for managing, handling and disposing of government information. An initial cross-government training initiative on roles and responsibilities associated with information and technology security, privacy and records management was developed by representatives from the OCIO, PSA and ministries.

The OCIO Report recommendations will be supported through content added and delivered through the training initiative to a variety of channels and various audiences within the public service. Specifically new content is being developed in support of the training provisions from recommendation 8.

Awareness themes include;

- Central government policy implementation is dependent on ministry level policy, procedure and process supports and compliance monitoring.
- Documentation of operational level policies, procedures, standards and business processes is a major goal in achieving a more mature organization.
- Appropriate policy and information management resources are key mitigation strategies to minimize inappropriate release of information.
- Technology's value is dependent on the value of the information it contains.
- Disposition of technology is dependent on ensuring secure disposition of information assets first.
- Technology that has the capacity to store information should not be recycled or resold without a formal risk assessment and records management review.

C. Revised Security Policy

Prior to the Tapes Incident, a project was underway to develop new CIO supplemental policy and procedures related to the CPPM Chapter 12 and additional security responsibilities of the

CIO. The project was designed to implement the ISO 17799:2005 Code of Practice for Information Security Management. The first iteration of this standard was released in July 2006 in the new Information Security Policy.

The new security policy provides a structured approach to identifying the broad spectrum of information management activities in the lifecycle of information systems. The policy further provides the framework for government organizations to establish local policies and procedures necessary for the protection of government information and technology assets.

The new policy has been communicated to the ministries and the OCIO Information Security Branch is working with ministries to begin implementation of the policies to improve security in managing information and technology. Implementation will provide more consistent protection across government. The OCIO is developing a Compliance Program associated with recommendations 2 and 3 to measure and report on corporate compliance with the new policy.

D. Resource Implications

The initial investigation and implementation of the OCIO Report recommendations incurred high time commitments and resource demands from the OCIO and ministries. Many of the activities that arose from implementing the recommendations will require ongoing staff effort over months to address concerns, design improved policies, procedures and business processes, and consult with ministries to arrive at best practices in the area of information and technology asset disposal.

The business of ministries and of government does not stop when something creates a systemic need for change such as in the case of this incident. What initially seemed focused on asset disposal, in turn, raised the need to address more general information and technology management issues.

The governance review noted in section A above addressed a number of IM/IT management issues within the government system. Making the new governance framework successful will require the full and ongoing support of government and executives. The executive level championing of raising awareness of the dependencies of information and technology policies, services and products, minimizing risks, promoting ongoing improvements and supporting appropriate resource allocation will result in greater security and privacy being realized throughout central agency and ministry information and technology management.

Furthermore, successful implementation of the framework will require a review of human resources in the areas of policy development, privacy, information management, compliance auditing, security, and other related areas to determine the appropriate balance of resources needed with effective and efficient risk/threat management.

Coordination and cooperation will be significant themes in trying to address these needs and challenges within funding and resource allocations.

Appendix A: Original Recommendations

The following 10 recommendations were presented in the original Tapes Incident Investigation Report.

1. Central Authority Accountability

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

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 judgment 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., BlackBerry™, 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.

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.).

2. 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.

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.

3. 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, labeling, storing or disposing of sensitive media or devices.

Appendix B: Office of the Information & Privacy Commissioner's Recommendations

The Privacy Commissioner's makes three recommendations in his report F06-01 *Sale of Provincial Government Computer Tapes Containing Personal Information* (March 31, 2006). These have been addressed through addressing the 10 recommendations in the CIO's report and through additional work being done on governance and training. The three recommendations can be found in section 3.5 paragraphs 121 to 125 of the Commissioner's investigation report. They are:

1. Centralize Authority and Policy

> [121] "In my view, a better approach would be for the CIO to review existing policy and then create a central policy with which all Ministries and provincial government agencies must comply." [122] "Oversight of compliance should be subject to monitoring by the CIO and to external audit and checking, by my office where necessary." [123] "The central direction should cover all aspects of the lifecycle of media containing personal information, including in relation to office moves and to secure disposal of media containing personal information."

2. Encryption of Personal Data

> [124] "I believe the government must move quickly, and with high priority, with a strategy for encryption of personal information."

3. Outsourced and Alternate Service Delivery Providers

> [125] "Although it should go without saying, the government must ensure that all service providers under outsourcing or alternative service delivery arrangements use information technology security measures, and operate under policies and procedures, at least as good as those that the government employs. Ministries should also ensure that they commit the resources necessary to monitor service provider compliance and should commit to enforcing their contractual rights when service providers fail to live up to their promises around personal information."

How the recommendations were addressed in the OCIO activities:

Centralize Authority and Policy

This is primarily being addressed through the work being done on governance as described in the Governance Framework section on page 10. It will also be addressed through the ongoing development of standardized processes (see recommendations 2 and 3 above) and central agency policies and directives (recommendations 1, 4, 6, 7 and 10 above).

Encryption of Personal Data

There are three approaches that are being employed; a) encryption approaches as discussed in recommendation 5 above, b) increased awareness and training as described in the Awareness and Training section on pages 10-11, and c) introducing an information security classification described in recommendation 1 above.

Outsourced and Alternate Service Delivery Providers

Current CPPM policy 6.3.2 c. states Ministries must negotiate arrangements in Service Level or other agreements as required, between the Parties to meet the historical ministry compliance with the Core Policy and Procedures Manual. CPPM policy 15.3. #9. further states Ministries are responsible for ensuring that security policy applies equally to contracted services when sensitive information and assets of the Province require safeguarding.

Although this area was not specifically addressed in the initial CIO's report it was raised during discussions with Ministries. Comments from the reviews included concerns not only with outsourced providers but also with shared services. Concerns arose mostly around responsibilities for and control of information assets residing with Ministries and non-ministry contracted resources and shared service providers responsible for and controlling the technology housing the information asset. It was recommended through the recommendation 8 review that standardized contractual language, policies, procedures and processes be considered in this domain. The OCIO will need to identify activity leads to discuss these suggestions within Labour and Citizens' Services over the next few months. Standardizing contractual language with supporting policies, procedures and processes will help to improve our ability to monitor and audit contracted and shared services agreements.