Performance Audits

2 Government-wide: Controls Over Disposal of IT Assets

Summary

Government does not have adequate data security and inventory controls to prevent sensitive information from being exposed when information technology assets are disposed of and sent for reuse elsewhere – primarily in the public education system.

Computers issued to government employees are not configured to encrypt the data on their hard drives. Chief Information Office staff told us they intend to do this, but they do not have an implementation plan or timeline for this project.

Government's inventory of information technology assets is not managed appropriately. Policies and procedures do not have enough detail to provide sufficient guidance in the protection of sensitive data and secure disposal of information technology assets. Responsibilities for tracking information technology assets are not adequately communicated; some departments do not track their assets even though they are responsible for the data stored in them. Government has no processes to maintain the accuracy of inventory records. The Inventory Control Policy does not reflect the current inventory management structure or the increased risks associated with IT assets. Reconciliations of physical IT assets to inventory lists are not performed. We identified computers on inventory lists that were very difficult to locate; in one instance the computer was not found.

Government does not have a complete inventory record of its information technology assets. Some departments purchase their own IT assets; others request them from the Chief Information Office. In 2012, Chief Information Office staff started recording the purchases they made and disposals they performed. The computers purchased prior to that time, as well as those not purchased by CIO, may not be recorded. Without changes to the inventory tracking process, it is possible that the inventory will never be the complete.

We identified deficiencies with the processes used to dispose of surplus computers. There is no validation that all computers sent for secure wiping were actually wiped. The Chief Information Office does not tag all computers that have been wiped to identify computers ready to be sent for reuse. We identified five computers designated for reuse that were not wiped; one of which contained sensitive information.

The software used to wipe hard drives is not meant for business use. It does not provide an audit record or validation that a drive has been successfully erased. The validation could be done manually, but it is not.

2 Government-wide: Controls Over Disposal of IT Assets

Background

2.1 There are numerous costs associated with the loss or misplacement of information technology (IT) assets in government. Examples include replacement cost, costs to set up and re-issue a replacement asset, and the cost of the loss of employee productivity. There may also be a risk of exposure of the data contained on that IT asset. If the lost asset contains sensitive information such as financial, health, education or legal records, especially if any can be attributed to specific individuals, an unauthorized disclosure of data could have significant ramifications, including legal costs and damage to reputation. Affected members of the public would also be at risk, the scope of which would depend on the information disclosed.

2.2 The risk of improper disclosure of sensitive information can be reduced by using multiple layers of security, which provides extra protection if one security measure fails. Examples include encryption, tracking the assets that contain the information and securely wiping hard drives before disposal. Encryption is the process of scrambling data so that it can only be decoded and read by someone with the proper password.

2.3 Proper inventory management for computers tracks all such assets throughout their lifecycle. This enables management to detect if data storage devices become misplaced. Key events and information that should be recorded include the following.

- Purchasing – the primary users and the serial numbers of new assets
- Maintaining – changes of owners, location or primary use
- Disposing – the date the asset is removed from service, steps taken to secure the data, and the asset's final destination

2.4 Data disclosure risks are further mitigated by securely wiping hard drives. Even though data may be deleted from hard drives by users, that information may be readable through the use of data recovery tools. Sanitization (secure wiping) of hard drives is meant to prevent recovery of such data. The Province requires all computer hard drives be securely wiped before releasing the computers for reuse elsewhere.

2.5 The Department of Transportation and Infrastructure Renewal has a central computerized inventory tracking application which can be used for IT assets throughout government. Transportation staff provide training to departments

choosing to use the application. They are also responsible for collecting and reporting annually on government inventory that has been deemed surplus.

2.6 The Chief Information Office (CIO) provides computer acquisition and disposal services to government departments as requested. If a department uses the CIO for acquisition or disposal, that action is recorded in Transportation's central inventory system.

2.7 CIO sends surplus computers to Computers for Schools. Computers for Schools is a nonprofit organization that accepts donations of computer equipment from various levels of government and businesses. Donated equipment is refurbished and distributed, mostly within the Nova Scotia public education system. According to a government news release, the list of donated equipment for fiscal year 2011-12 included 1,381 desktops, 270 laptops, and hundreds of accessories such as keyboards, monitors, printers, speakers and computer mice.

Audit Objective and Scope

2.8 In the summer of 2013, we completed an audit of controls over secure disposal of information technology assets. The objectives of our audit were to:

- assess the adequacy of internal controls in core government to appropriately manage the inventory of information technology assets; and
- assess the adequacy of internal controls in core government to ensure sensitive information has been securely deleted from specified information technology assets before their reuse or disposal.

2.9 Devices in use by government which may contain sensitive data include the following.

- Computer hard drives
- Server hard-drives and network-attached storage devices
- Photocopiers and printers
- Smartphones and tablets
- USB drives

2.10 We considered the risk of data loss and decided to focus our audit testing mainly on computer hard drives and smart phones.

2.11 Audit criteria were developed specifically for this engagement using both internal and external sources. We examined policies, processes and controls within Transportation and Infrastructure Renewal and Chief Information Office to manage the inventorying, secure wiping, and disposal of information technology assets. We tested IT asset inventory practices at a sample of departments: Health and Wellness, Justice, and Community Services.

2.12 The audit objectives and criteria were discussed with, and accepted as appropriate by, members of management responsible for the systems we audited.

2.13 Audit fieldwork was conducted in accordance with Sections 18 and 21 of the Auditor General Act and auditing standards adopted by the Chartered Professional Accountants of Canada. We carried out fieldwork between October 2012 and May 2013 on IT process transactions that occurred between January 1, 2012 and December 31, 2012. Adequacy of controls over disposals was assessed at various points throughout fieldwork.

Significant Audit Observations

Encryption

Conclusions and summary of observations

Information contained on provincial government laptop and desktop computer hard drives is at an unnecessarily high risk of improper disclosure. Computers used by government employees do not have data on their hard drives encrypted and the Chief Information Office has not established a timeline to implement encryption.

2.14 *Computer hard drives* – Currently, laptop and desktop computers used by provincial government employees do not have encrypted hard drives. If these devices are misplaced, unauthorized individuals could read the hard drives, which may expose sensitive information. The Chief Information Office intends to encrypt the data on all government computer hard drives, but has not established a timeline or implementation plan. Therefore, reliance is mostly placed on the inventory management process to account for IT assets and the process of securely deleting the information contained in them upon disposal.

Recommendation 2.1
The Chief Information Office should ensure all computers issued to government employees are configured to encrypt their data.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation and intends to encrypt the data on all computers issued to government employees. An implementation plan will be developed to determine the timeline and any funding requirements and human resource implications.

2.15 *Smartphones* – The Province will only allow government-issued Blackberry smartphones to connect to the provincial network. Upon activation, these devices download a security policy which encrypts the device and requires a password at all times. These Blackberries can be wiped remotely if lost or stolen and have a password attempt limit of 10 before triggering an automatic wipe of the device. These security features mitigate the risk of data loss on government smartphones.

2.16 We found surplus smartphones awaiting destruction at the government surplus warehouse. We tested 46 phones and only found four that were not locked. These smartphones were in service before passwords were mandatory. We found emails stored on them. However, in turning the smartphones on, they connected to government computers which triggered an automatic wipe. None of the information could then be retrieved.

Information Technology Inventory Management

Conclusions and summary of observations

Information technology inventories are not adequately managed, increasing the risk of sensitive information stored on those devices being inadvertently exposed. Government does not have a complete and accurate record of all of its information technology assets. We found inaccuracies in each of the inventory lists we tested. Departments are not reconciling physical IT assets to asset lists. Further, accountabilities for information technology asset inventory management have not been communicated.

2.17 *Background* – IT asset inventory management is the process of tracking and accounting for all significant IT assets throughout their lifecycle. When new IT assets are purchased, the documentation to support the purchase should be retained and certain information about the asset should be recorded, such as serial number, its location, and to whom it was issued. If IT assets change location or owner, inventory records should be updated. Departments should periodically reconcile physical assets to inventory listings to ensure records are accurate and all assets owned are accounted for. When an IT asset is at the end of its useful life, stored data should be securely wiped before the asset is discarded and inventory records should be updated to reflect this important safeguard.

2.18 *Responsibilities for IT inventories* – The government's Information Management Policy stipulates that departments are responsible to protect information contained on their IT assets. Departments are also charged with tracking assets, including IT equipment, as noted in government's Inventory Control Policy. Currently, CIO staff only record IT asset purchase and disposal information. Once deployed, tracking the asset and the data on it become the responsibility of the receiving department. We found that none of the departments we tested knew it was their responsibility to keep this information up-to-date. There is no clear understanding by all parties as to who is responsible for which aspect of inventory tracking. This is discussed in greater detail in the Inventory Legislation and Policies section later in this chapter.

2.19 *Departmental processes* – There is a government-wide electronic inventory system available to all government departments, agencies, boards and commissions to use in tracking their capital asset inventory. The Department of Transportation and Infrastructure Renewal provides training to departments upon request, but departments are not required to use this application to track their assets.

2.20 In 2012, CIO began using this centralized inventory system to record all IT asset purchases made on behalf of departments. Since assets purchased earlier may not be recorded in the system, and because departments are not required to purchase IT assets through CIO, it is possible that the inventory listing may never be complete.

2.21 CIO has an on-line process through which most departments order computers. However, not all departments purchase computers through CIO. Of the three departments we examined, both Health and Wellness, and Justice utilize CIO's purchasing service. The Department of Community Services manages its own IT inventory, including purchasing.

2.22 The Department of Health and Wellness relies on the CIO to purchase and dispose of its computers, and to record those activities in the centralized inventory system. The Department does not track its own inventory of computers and relies on reports provided by CIO. Those reports are based on identifying computers that have connected to the provincial network in the last 120 days. If there are computers which have not been connected to the network during this time period, the list will not be complete. This identification method cannot be relied upon as an accurate method of inventory management.

Recommendation 2.2
The Department of Health and Wellness should develop and implement a process to ensure its information technology asset inventory records are complete and accurate.

Department of Health and Wellness Response:
The Department of Health and Wellness is in agreement with the recommendation and will work in conjunction with other key departments including the Department of Transportation and Infrastructure Renewal and the Chief Information Office to develop and implement a process to ensure its information technology asset inventory records are complete and accurate. The Department of Health and Wellness expects to have this in place by November 2014.

2.23 Currently, the CIO maintains records of Justice's IT asset purchases and disposals in government's central inventory system. Prior to 2013, the CIO maintained a separate inventory database for that Department's IT assets. The database was owned and maintained by Justice until the CIO was established, at which point the CIO continued to maintain the database. The database will be phased out when the assets recorded in it reach the end of their lifecycle. We tested the accuracy of both the database and the central inventory list. We found that neither inventory was accurate.

- 18 of 20 sample assets which were removed from use per the Department's database had not been recorded as such in the central inventory list.
- Six of 10 sample purchases made between April and December 2012 were not recorded in the Department's database.

Recommendation 2.3
The Department of Justice should develop and implement a process to ensure its information technology asset inventory records are complete and accurate.

Department of Justice Response:
The Department of Justice will work with both the Chief Information Office and Transportation and Infrastructure Renewal to improve the way information technology assets are tracked. The Department will implement a policy requiring divisions to keep a master list of Blackberries and cell phones authorized for use by staff and record when the asset is replaced and the old asset destroyed or returned for surplus. In addition, a policy will be implemented addressing the process to be followed when assets are replaced, either through Evergreen or one off replacements, and the removing of assets from the network. The Department of Justice expects to have this in place by the end of the current fiscal year.

2.24 The Department of Community Services does not use the CIO to purchase its IT assets, and it does not use the central inventory system to track them. The Department retains purchase orders, packing slips and invoices in binders for each fiscal year, and the assets procured and disposed of are tracked in spreadsheets. The Department does use the CIO disposal service for its computers.

2.25 While Community Services does have a process to track its IT assets, we noted the following issues with the spreadsheet used to record this information.

- 2 of 20 sample purchase orders were not recorded.
- 8 of 20 sample computers connected to the Department's networks were not recorded.
- 1 of 20 sample purchase orders tested was incorrectly recorded.
- Serial numbers were not recorded for 40 assets in the system.

Recommendation 2.4
The Department of Community Services should develop and implement a process to ensure its information technology asset inventory records are complete and accurate.

Department of Community Services Response:
The Department of Community Services agrees with this recommendation and will work with the Chief Information Office to implement a process that will ensure the Department's information technology inventory records are complete and accurate from time of procurement to disposal. This work will be completed within this fiscal year.

2.26 *Inventory reconciliation* – Based on our testing and discussions with management at Transportation and Infrastructure Renewal, departments are not reconciling their IT assets and inventory records. We selected a sample of computers from inventory listings and attempted to physically locate them. We identified one computer purchased by the Department of Community Services and four by the Department of Justice that could not be readily located. Four of the computers were eventually found; one was never located. If that asset was not processed through government's secure disposal procedures, there is an increased chance that the hard drive has not been securely wiped. The lack of reconciliations increases the risk that IT assets with sensitive government information have been disposed of without securely wiping the hard drive and that information could be exposed. All departments should be required by government policy to reconcile their IT inventory lists to the actual items on hand. This is addressed later in this chapter.

2.27 *Smartphones* – Smartphones are used throughout government and have the capacity to hold large amounts of sensitive information, such as emails and related attachments. We found that departments have varying processes to manage smartphone inventories. However, security features are enabled on all devices which mitigates the risk of data loss. It is expected that recommendations made in this chapter to improve information technology asset inventory processes would include smartphone assets, providing further protection for government data.

Inventory Management Software – Application Controls

Conclusions and summary of observations

The applications used by the Department of Community Services and the Department of Justice do not have adequate application controls to maintain the accuracy of the inventory records contained within them. The inventory system provided by the Department of Transportation and Infrastructure Renewal and used by the Chief Information Office has some controls, however additional safeguards should be in place.

2.28 *Inventory applications controls* – Inventory tracking systems used by departments should have safeguards to restrict what users can do within the application. These are commonly referred to as application controls. This enables management to rely on the accuracy of information in the application. If users are able to delete or modify records without authorization, they could potentially change details about inventory items or remove IT assets without being detected.

2.29 We assessed the systems used by our sample departments against application controls we would expect to be in place to protect the accuracy of data. Based on this assessment, we found inventory applications did not have adequate controls. Application controls should be implemented to mitigate risks relating to the accuracy of data in the inventory applications we examined. The table below summarizes our testing results.

Application Control	Transportation and Infrastructure Renewal Centralized System	System Used by Department of Community Services	System Used by Department of Justice
Users are required to authenticate themselves through a username and password	✓	✓	X
User accounts are locked out if username or password attempts are invalid after a specified number of times	X	X	X
Permissions can be assigned to restrict access to functions such as creating, modifying and deleting records	✓	X	X
Logs are generated when a user creates, updates, transfers or deletes a record	X	X	X
User accounts expire or are disabled after a period of inactivity	X	X	X
Passwords are required to be changed periodically	X	X	X

2.30 As discussed earlier, the Department of Justice's inventory system is being phased out as it transitions to Transportation and Infrastructure Renewal's central inventory system. New inventory is not recorded in the old system. Accordingly, we do not recommend any changes to this system.

Recommendation 2.5
The Department of Community Services should utilize an inventory management application that prevents unauthorized access through strong password control; prevents authorized users from performing unauthorized transactions; logs all user activity; and disables accounts when they become dormant.

Department of Community Services Response:
The Department of Community Services accepts this recommendation and will transition to use the Department of Transportation and Infrastructure Renewal's centralized inventory management system that meets most of the application controls outlined in this report. This work will be completed within the fiscal year.

Recommendation 2.6
The Department of Transportation and Infrastructure Renewal should administer a central inventory management application that prevents unauthorized access through strong password control; prevents authorized users from performing unauthorized transactions; logs all user activity; and disables accounts when they become dormant.

Department of Transportation and Infrastructure Renewal Response:
The Department of Transportation and Infrastructure Renewal agrees with the recommendation of the Auditor General. The Department will be upgrading to the latest version of Archibus V21.1 which will address the issues raised.

Information Technology Asset Disposal

Conclusions and summary of observations

Standards related to information security need improvement and procedures for information technology asset disposal should be documented. There are weaknesses in the process to wipe hard drives, including use of inadequate software, lack of identification labels for wiped computers, and no verification that computers have been wiped. Departments are not listing the computers they need wiped by CIO and they do not receive any documentation back as to which computers were wiped. More detailed information needs to be recorded in the inventory records for disposed assets and additional procedures are needed to ensure all disposals are recorded.

2.31 *Secure disposal* – When a provincial government IT asset is declared surplus, the government's Wide Area Network Security Policy and supporting standards require any sensitive information on it to be deleted in a secure manner. However, there is no indication which asset categories are covered by the policy. Additionally, it does not refer to government's Information Management Policy which requires departments to classify information into its various types as well as safeguard information from improper disclosure, use, disposition and destruction.

Recommendation 2.7
The Chief Information Office should modify the standards that support the Wide Area Network Security Policy to indicate the categories of information technology assets covered by the policy and to reference its relationship to government's Information Management Policy.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation. The Chief Information Office understands that updating the Wide Area Network Security Standards will address this recommendation. This is already in process.

2.32 CIO IT asset disposal services are available to all provincial departments. Government policy requires all electronic storage devices to be securely wiped. If hard drives cannot be securely wiped, they must be destroyed. Departments are to notify CIO when there are IT assets to be disposed of and a staff member from CIO performs the secure wipe. The wiped computers are sent to Computers for Schools (see Background section). Hard drives that cannot be wiped (e.g., nonfunctional drives) are removed and sent for destruction at a metal shredding facility. Currently, smartphones also must be shredded because they cannot be reused for security reasons.

2.33 While there is a process for secure IT asset disposal, it is not documented. Written procedures are necessary to ensure consistency of processes and continuity in the event of the departure of key staff members. Departments using CIO's disposal service should be provided information on the secure wipe process and related responsibilities. This would assist them in fulfilling their responsibility to protect the security of the sensitive information they handle.

Recommendation 2.8
The Chief Information Office should document its information technology asset disposal process indicating the procedures, responsibilities and service contacts involved. This documentation or a summary of it should be provided to departments that use the Office's disposal service.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation. Work is already underway in documenting the procedures, responsibilities, and service contacts for the asset disposal service.

2.34 *Secure wiping* – Secure wiping of hard drives (digital sanitization) is especially important because government hard drives are not encrypted and therefore do not have the first layer of data security discussed earlier in this chapter. We assessed the CIO's process to securely wipe information from hard drives and noted the following deficiencies.

- The software used by the CIO is not intended for business use and does not maintain logs, leaving no means of validating that a hard drive was wiped or to assist when investigating a data security breach.
- There is no standard identification method (e.g., label) to indicate that a device has been successfully wiped.
- There is no periodic verification that computers sent for disposal were wiped.

2.35 We tested a sample of 100 computers that were designated as surplus and therefore should have had their hard drives wiped. Five of these computers contained information which was easily readable, proving they had not been wiped. One contained sensitive information, including recorded 911 calls, very personal details relating to a background check, and other personal information. These computers would have been sent to Computers for Schools, with sensitive information still accessible.

Recommendation 2.9
The Chief Information Office should use sanitization (secure wiping) software that records and reports information on wipe processes and results.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation. The Chief Information Office will investigate a solution for sanitization with appropriate audit and reporting capabilities. An implementation plan will be developed to determine the timeline and any funding requirements and human resource implications.

Recommendation 2.10
The Chief Information Office should implement a standard procedure that provides a visual identification of whether information technology assets have been wiped.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation. Changes are being implemented to the existing processes to ensure hard drives that have been wiped are clearly identifiable.

Recommendation 2.11
The Chief Information Office should periodically verify that computers sent for disposal were wiped.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation. Procedures are being modified to provide for periodic verification that computers sent to the Chief Information Office for disposal were wiped in accordance with the Chief Information Office policy and procedures.

2.36 *Destruction of data storage devices* – Data storage devices that cannot be securely wiped are required to be physically destroyed. The destruction process is witnessed by a CIO employee and photo evidence of the destruction is retained.

2.37 Departments can choose to have their hard drives destroyed instead of reused. This is the case at the Department of Justice for computers and other devices used by judges and their support staff. Justice requires that all hard drives from these devices be removed and physically destroyed upon retirement of an asset. The hard drives are removed by CIO, and left behind with the users. Those hard drives are stored in a safe until they are taken for shredding. We observed hard drives in the safe as part of our audit testing.

2.38 *Documentation of disposals* – CIO updates the centralized inventory system after it performs its disposal procedures for departments. We found that inventory records accurately reflect the device details and locations, but do not indicate whether the devices were securely wiped and related details. We tested 80 computers and found the following.

- Asset description details in the centralized inventory system were accurate for all 80 computers tested (e.g., tag numbers, computer description, serial numbers, current location).
- Inventory records did not indicate whether devices had been securely wiped for 58 of 80 computers tested.
- Of those that were indicated as being wiped, only one provided a date for the procedure.
- The inventory records did not indicate who performed the secure wipe or if anyone confirmed that the procedure occurred.

2.39 As noted, the Department of Community Services uses its own inventory system, but relies on CIO for disposal services. We tested a sample of 20 of the Department's IT assets on which CIO was to have performed disposal procedures. We noted that 14 of those items did not have the disposal details recorded. Of the six that were recorded, five were noted as surplus, but none indicated if the drives had been wiped.

Recommendation 2.12
The Chief Information Office should develop a process to ensure all the information technology asset disposals it performs are recorded in a centralized tracking system.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation. A centralized spreadsheet has been developed and is being deployed to track the asset disposals.

Recommendation 2.13
The Chief Information Office should retain specific disposal details for each asset it services such as sanitization (secure wipe) status, date of disposal, the individual who performed the disposal procedures, and current location.

Chief Information Office Response:
The Chief Information Office agrees with this recommendation. These specific data elements will be captured in the centralized tracking spreadsheet.

2.40 *Tracking of disposals* – When departments upgrade their IT assets, the assets leaving the department are collected and CIO is then responsible for secure wiping. Departments are not providing CIO with a list of assets expected to be wiped, and CIO does not provide departments with a list of devices wiped. Considering the weaknesses we identified in tracking and secure wipe processes, there is a risk that an asset with sensitive information is unknowingly lost in transit to its final destination, resulting in a greater risk of sensitive information not being wiped. This is another reason that the government's Inventory Control Policy should include reconciliations between physical IT assets and asset listings, as discussed below.

Inventory Legislation and Policies

Conclusions and summary of observations

The Inventory Control Policy does not reflect the current inventory management structure or risks associated with IT assets. The policy does not provide

sufficient descriptions of the assets to which the policy applies, nor does it assign responsibilities for tracking assets through their lifecycles.

2.41 *Inventory control policy* – According to current policy, Transportation and Infrastructure Renewal is responsible to monitor the use, distribution, and disposal of capital assets, including IT assets, across government. The Inventory Control Policy requires all departments, agencies, boards and commissions to provide annual reports to Transportation and Infrastructure Renewal detailing additions and deletions to capital asset inventories during the year. We reviewed the policy and determined it does not reflect the current structure of inventory management across government. The wording in the policy reflects a centralized inventory management process administered by Transportation and Infrastructure Renewal. However, the inventory function was decentralized to departments a number of years ago.

2.42 In discussing the Inventory Control Policy with Transportation and Infrastructure Renewal officials, a number of weakness were identified that may contribute to many of the concerns we expressed earlier in this chapter regarding IT inventory control.

- The policy does not assign responsibility to departments and agencies to check inventory lists against actual inventory.
- The policy does not assign responsibility to any organization to check that inventory lists are maintained and reconciled.
- The policy does not assign responsibility to ensure that IT assets which are disposed of are appropriately controlled through the disposal process.

2.43 We also noted that the policy does not provide sufficient description of the types of assets to be inventoried and controlled. By default, almost any physical item can meet the current description, resulting in inventory lists which are too large to maintain and reconcile in an economical manner. A policy focused on items of particular risk of loss (e.g., technology, expensive assets, easily portable or concealable items) would be less costly to manage and control and would likely result in better compliance with inventory control requirements.

2.44 Addressing the weaknesses in the current policy would impact all physical assets of government, including IT assets, and therefore would strengthen the controls over those IT assets and the information they contain.

Recommendation 2.14
The Department of Transportation and Infrastructure Renewal should work with Treasury Board Office to update the Inventory Control Policy to reflect the current inventory management structure and processes. The policy should contain a definition of which assets to list and control; assignment of responsibilities to control inventories; a requirement to maintain accurate and complete inventory records which are reconciled to physical assets on a regular basis; processes for secure disposal of replaced assets; and responsibilities for enforcement of the requirements of the updated policy.

Department of Transportation and Infrastructure Renewal Response:
The Department of Transportation and Infrastructure Renewal agrees with the recommendation of the Auditor General. The Department will develop a new Inventory Control Policy in conjunction with Treasury Board, the CIO and other key departments to address the issues raised.

2.45 The Surplus Crown Property Disposal Act requires departments to provide annual reports to Transportation and Infrastructure Renewal, including particulars on surplus assets disposed of during the year. We found departments are meeting this requirement. However, departments are relying on the CIO to record details of surplus computers at the time of disposal to ensure compliance with the Act. Without adequate inventory tracking of IT assets deployed across government, it is impossible to determine if all applicable assets have been identified and included in the surplus reporting process. Once the recommendations made as part of this audit are implemented, more assurance can be placed on the annual surplus reports.