Audit of Tax Data Security

Final Report
Approved by Internal Audit Committee on June 29, 2005

Audit and Evaluation Division
March 2005

Statistics Canada Statistique Canada

Canada

Table of Contents

Auditor's Statement **1**

I. Introduction **2**

II. Findings and Recommendations **2**

III. Conclusion **7**

Appendix A—About the Audit **8**

Objectives 8
Scope 8
Criteria 9
Methodology 9

Appendix B—Management Action Plan **11**

Auditor's Statement

We have completed the Audit of Tax Data Security, the objectives of which were: to identify the extent to which tax data user divisions comply with the conditions in the Memorandum of Understanding between Canada Revenue Agency and Statistics Canada and relevant Statistics Canada policies and practices concerning the use, security, retention and disposition of tax data; and the extent to which external communication of tax data to others is managed in accordance with the Agency's *Discretionary Release Policy* and associated guidelines. The audit was to identify measures to improve practices.

This internal audit was carried out in accordance with the Internal Auditing Standards for the Government of Canada. Key activities during the audit period focussed on 12 divisions using tax data, included inspecting 332 offices in 8 of these divisions, interviewing approximately 130 Statistics Canada employees working in 15 divisions (the 12 just referred to, plus 3 divisions providing services), observing practices and reviewing documents.

In examining Statistics Canada's compliance with the requirements of the tax data Memorandum of Understanding between it and the Canada Revenue Agency, we are satisfied that the care demanded for tax data is being provided in the divisions examined, subject to the exceptions noted. The main exception is the improvement recommended to better secure tax data transported in Statistics Canada's care. Taking these additional steps would help protect our reputation if an incident were to occur, however remote the chance.

These conclusions are based on the assessment of findings against pre-established criteria and agreed to by the Internal Audit Committee in April 2004 and reflect the audit work conducted principally between May 2004 and January 2005.

In my opinion, sufficient and appropriate audit work has been performed and evidence gathered to support the conclusions contained in this audit report.

Beverly Prentice
Audit Manager

March 2005

I. Introduction

To produce some of its statistical information, Statistics Canada uses tax data provided by Canada Revenue Agency[1]: tax data are a significant and growing source of administrative data. A Memorandum of Understanding was signed April 4, 2003 between Statistics Canada and Canada Revenue Agency, replacing a number of earlier agreements and setting out the conditions under which tax data are provided to Statistics Canada. In addition, Statistics Canada depends on the cooperation of the Canadian public for its success. Security measures related to confidential information protect our reputation.

The memorandum places certain stipulations on Statistics Canada with respect to the handling, security and use of Canada Revenue Agency information. One condition requires Statistics Canada to conduct audits focussing on the extent to which it adheres to the terms and conditions related to: the use; security; retention and disposition; and the provision of tax data to others under the *Income Tax Act*, *Excise Tax Act* and the *Statistics Act*. This report presents key results of the first audit, conducted within the agreed two year time frame.

A large number of divisions use tax data—when the memorandum was signed there were 37. We updated and selected a sample, so the audit results presented in this report are based on this sample. Methodological details are provided in Appendix A.

II. Findings and Recommendations

Overall, we are satisfied, subject to specific exceptions noted, that Statistics Canada is taking care of the tax data entrusted to it, in keeping with the conditions in the Memorandum of Understanding (MOU) and departmental policies and procedures underpinning it[2]. Tax Data Division tracks uses and users and all divisions examined control electronic access. Information technology and physical security requirements are being met for the most part, but we recommend improvements when transporting tax data and sanitizing computers. Retention and disposal are handled appropriately. Providing tax data to others is in accordance with the Statistics Act and Statistics Canada's *Discretionary Release Policy* and associated guidelines.

We provided divisional results to directors through management memos and plan to monitor their actions. Most are simple to execute and we have had excellent cooperation. Already, most divisions have indicated that they have addressed the recommendations even though we have not begun the monitoring phase yet.

We gathered promising practices from divisions and have compiled a general list suitable to share with all divisions where sensitive statistical information resides, not just tax data.

[1] When the MOU was signed, the agency was known as the Canada Customs and Revenue Agency.
[2] Relevant policies and procedures are: *EDP Security Policy*, *Policy on the Security of Sensitive Statistical Information* and the *Security Practices Manual*.

Tax Data Division tracks users and uses

Tax Data Division (TDD) has taken a leadership role in promoting best practices concerning tax data security, reflecting its unique responsibility within Statistics Canada as the primary source of tax data. Then other divisions access those parts of the tax databases relevant for their specific uses, once TDD has readied the data. TDD maintains a system to give electronic access only to those authorized by their directors to have access to tax data under its control. It is based on user request forms that indicate the use being made of the data, the time period for which this is necessary and contains a declaration that users sign concerning the conditions they will meet. This demonstrates that the 'need to know' principle is applied.

By monitoring users and uses from its systems information and the forms, Tax Data Division has the capacity to track changes. Divisions understand their uses and how they are changing and therefore are well-positioned to assist Tax Data Division when it refreshes this information. The MOU is a living document with provisions for updating. Tax Data Division maintains a working relationship with Canada Revenue Agency; part of this involves refreshing information on tax data files and their uses.

Tax Data Division has made a template of a form available for other divisions to use as circumstances warrant. Take-up is good and the form applies beyond a tax data context. It helps divisions meet their obligations to record inter-divisional use of sensitive statistical information (including tax data) under the *Policy on the Security of Sensitive Statistical Information*.

Divisions control electronic access

In the case of inter-divisional access, both the director from the division having custody of the tax data and the director of the recipient division give their approval, as required by the *Policy on the Security of Sensitive Statistical Information*. While mechanics differ, their effect is to provide a systematic control on who obtains access. Divisions give their own employees access to tax data on the basis of a supervisor's verbal or e-mail request.

Tax Data Division has recently modified its request form to provide space to document users within a division having access to tax data. This covers those circumstances where a limited number of users get access through Tax Data Division and import it into their own division for use by a larger number of employees. This creates historical documentation and complements a division's ability to identify current users.

Improvement possible by removing access faster

Access needs to be removed when employees no longer require it. Statistics Canada has corporate controls through the employee clearance form to remove access to its internal corporate-wide network—'Net A'—when an employee leaves. Similarly, when

employees change divisions, 'Net A' needs adjusting. LAN administrators update its corporate directory, also called 'active directory'. While we did not test the effectiveness of these controls, we did assess internal divisional practices.

Making these network changes does not remove access to independent divisional systems. However, divisions have mechanisms to remove access to these systems under their control, usually on a periodic basis, e.g., yearly. In a couple of divisions, this task has been automated and can be done easily on a more frequent basis. In brief, processes use corporate information in 'active directory' and compare it to the independent divisional system information. Where there is no match, immediate action can be taken. For example, if the corporate directory shows the employee now works in another division, but still has access to the independent divisional system, then that access can be removed. Although we are not proposing a formal recommendation, we suggest that building on this experience elsewhere would improve this capacity.

Electronic security requirements met

Tax data are stored with appropriate access controls such as passwords and permissions in place. In the occasional case where folders had permissions that were not sufficiently restrictive, corrective action was taken immediately.

Physical security OK

We found that tax data was properly stored in 88% of the offices examined. In five of the eight divisions inspected, we found no storage problems related to tax data. The remaining three accounted for nearly all of the 12% of offices where tax data were left out overnight. Directors responsible have taken corrective action. For this subset group, half were in one division where an incorrect procedure was the cause and this has been corrected since. We also observed that in this subset group, we found the material in unlocked shred boxes in half the cases and suggest that shred boxes not be used.

Similar cases could exist in divisions outside the sample, or in other divisions handling sensitive statistical information that is not tax data. We suggest that these directors verify that employees are properly storing sensitive statistical information.

We found divisional servers containing tax data physically restricted within divisional or main computer centre control. A/B switches were not used by tax data users nor did they have personal digital assistants connected to network A.

Tax data are retained and disposed of appropriately

We focussed mainly on disposal practices. Electronic files held on the mainframe are released according to procedures that make it impossible to reconstruct data. Some divisions have shredders to shorten the time between creation of a paper document and its destruction. This eliminates additional handling and consequently reduces risk. While they do not apply exclusively to tax data, clean-up days are regularly scheduled in some divisions, providing another disposal opportunity.

Transmitting tax data between Canada Revenue Agency and Statistics Canada needs improvement

Canada Revenue Agency regularly forwards tax data in various forms (tape, CD, paper) to Statistics Canada. A courier company is routinely used by Canada Revenue Agency to get selected items to Statistics Canada. Most others are picked up by Statistics Canada drivers and in the case of tapes, returned by driver. This is accomplished through 'runs' which involve multiple stops, including Canada Revenue Agency.

- **Better Statistics Canada procedures**

Runs by Statistics Canada drivers with no stops in-between would contribute to better tax data security wherever it could be achieved. Striking a balance between security and workable operations is necessary. There are some opportunities for Statistics Canada to improve transmittal security with little effort.

The MOU lists three essential elements for Statistics Canada to follow when transmitting protected information—package to prevent damage; double-envelope and label properly; and for removable media, apply regional office guidelines that require a locked outer layer when shipping. There is ambiguity about the circumstances under which the regional office guidelines for locking apply and this should be removed, preferably by establishing specific requirements for transport using SC drivers.

We were told that packaging was sometimes an issue, although it is not possible to adequately describe or quantify, since Statistics Canada did not keep records of these events. This makes it impossible to know what the specific problem was, how often it occurred, when follow-up, if any was done, and by whom. We recommended in a management memo that such records be kept. Statistics Canada needs to take action to protect its reputation if an incident, for example a theft, tampering or accident, were to occur, however remote the chance.

> ***Recommendation:*** Tax Data Division consults with Administrative Support Services Division (service provider for drivers) to explore options for direct transport and find ways to improve packaging and include these in its procedures manual. The procedures manual should include a process to identify and log any incidents related to packaging or transport, and report them to divisional management so that appropriate action can be taken. This will provide procedures tailored for these circumstances.

- **Harmonization of transmitting standards**

There is no clause in the MOU obligating Canada Revenue Agency to follow the standards expected of Statistics Canada. It is important to remember that these standards are higher than the minimum government standard for transmitting 'protected B' information—a single sealed envelope—which is the standard for Canada Revenue Agency. Since the Statistics

Canada standards protect tax data against a risk that is independent of the sender, seeking Canada Revenue Agency buy-in to revise the MOU so that both parties work to the same standard would be beneficial.

> ***Recommendation:*** Tax Data Division works to revise the MOU so that what is expected when Statistics Canada drivers transmit tax data is clarified.

Need to sanitize computer hard drives with the latest software

Whenever a computer leaves Statistics Canada for re-use (e.g., computers for schools program), the division discarding it is responsible to sanitize it by using DSX software from the RCMP and choosing the 'three-pass' option rather than the 'one-pass' option, as the RCMP recommends. Typically, LAN staff does this. We found old versions of the software widely in use and the three-pass option was not always chosen. The most recent version of the software was not available within Statistics Canada when we checked, although this was immediately rectified when pointed out.

Administrative Support Services Division (ASSD) verifies that computer hard drives have been sanitized before leaving Statistics Canada, although it is technically not possible to check that the three-pass process was used. ASSD was not checking that the correct version is used. We raised this with the director, who has indicated since that: the newest version has been provided to the Quality Control area; and that clients will be advised if they are not using the appropriate version. We informed those divisions where we conducted our debriefing after this problem was identified and have alerted all Field IT Service Managers. Directors have responsibility to ensure that security is properly handled within their divisions, and helping service providers to take appropriate action will assist them.

> ***Recommendations:*** Informatics Technology Services Division keep the most recent version of the sanitization software package available on its website and notify Field IT Service Managers so that they take steps to ensure that employees reporting to them sanitize computer hard drives leaving Statistics Canada using the latest version; and that ITSD also notify the Supervisor Assets Management / Quality Control in Administrative Support Services Division.

Providing tax data to others handled appropriately

Statistics Canada follows its *Discretionary Release Policy*; tax data are provided to others according to the permitted conditions. Informatics Technology Services Division has conducted site inspections to ensure that security measures are in place before data are sent. Reports summarizing results have been provided to the Director of Tax Data Division. A checklist is used to guide the inspection work.

We focussed on the five memorandums of understanding signed between the statistical agencies of the four western provinces and Quebec, where tax data are being provided.

These MOUs[3] include conditions that require the recipients to care for the data to the same standard expected of Statistics Canada. They have been given assistance to understand what is required via meetings and presentations. This is in addition to the MOUs themselves, which include Statistics Canada's *Policy on the Security of Sensitive Statistical Information* so that recipients can extract relevant principles, along with specific standards copied from the Canada Revenue Agency–Statistics Canada Memorandum of Understanding.

III. Conclusion

In examining Statistics Canada's compliance with the requirements of the tax data Memorandum of Understanding between it and the Canada Revenue Agency, we are satisfied that the care demanded for tax data is being provided in the divisions examined, subject to the exceptions noted. The main exception is the improvement recommended to better secure tax data transported in Statistics Canada's care. Taking these additional steps would help protect our reputation if an incident were to occur, however remote the chance.

[3] Those pertaining to section 17(2)(a) of the *Statistics Act* and section 241(4)(o) of the *Income Tax Act*, permitting disclosure for research and analysis where the agency is authorized by law to collect the same information

Appendix A—About the Audit

Objectives

The audit assessed

- the extent to which tax data user divisions comply with the MOU and relevant Statistics Canada policies and practices concerning the use, security, retention and disposition of tax data within Statistics Canada
- the extent to which external communication of tax data to others is managed in accordance with the *Discretionary Release Policy* and associated guidelines

Scope

Section 34 of the MOU directs Statistics Canada to "…conduct periodic internal audits of their use, provision of tax data to others[4], security, retention and disposition with respect to protected client information." The audit covered all four areas:

Use

Annex C of the MOU provides a list of tax data files and brief descriptions of these general uses. The audit accepted these as given and focussed on management controls in place to keep information on use current. Use implies users and therefore an examination of the authorization to use tax data was included in scope.

Providing tax data to others

Under certain circumstances, the *Statistics Act* allows sensitive statistical information to be disclosed at the discretion of the Chief Statistician. Pertaining to tax information, one exception permits the disclosure of limited information in the form of an index or list of establishments under section 17(2)(f) of the *Statistics Act* and section 241(4)(d)(ix) of the *Income Tax Act*. The second exception is under section 17(2)(a) and a new provision under section 241(4)(o) of the *Income Tax Act*. This permits business-related tax information to be given to provincial and territorial statistical agencies for research and analysis where the agency is authorized by law to collect the same information. The audit focussed more on the second exemption.

Security

The audit included confidentiality aspects of IT security and physical security: focussing within divisions, not on building security or on cabling and wiring infrastructure. It excluded personnel security.

Retention and disposition

The audit focussed on the retention and disposal of tax files by divisions that are required to ensure that confidentiality is protected. It did not consider longer-term disposition matters such as archiving of records.

[4] The MOU uses the phrase "communication to others".

Criteria

We expected to find management practices and controls in place so that:

Uses

- Access to tax data is restricted to authorized individuals with a 'need to know'
- Tax Data Division tracks uses and users

Providing tax data to others (external)

- Procedures described in the *Discretionary Release Policy* and guidelines are followed
- Steps are taken to ensure that tax data provided to others are protected to the same level expected of Statistics Canada

Security

- Physical security requirements are met
- Information technology security requirements are met

Retention and Disposal

- Paper and electronic media are retained appropriately, excluding the requirement to mark every page
- Paper and electronic media are disposed of appropriately

These general criteria reflect terms and conditions in Annex D of the MOU, Statistics Canada policies and practices, and the *Government Security Policy*. The stewardship described in the MOU is generally the same as Statistics Canada standards for any sensitive statistical information.

Methodology

Twelve subject-matter divisions in four fields were selected for audit:

- Field 4—System of National Accounts: Income and Expenditure Accounts, and Environment Accounts and Statistics (N=2)
- Field 5—Business and Trade Statistics: Distributive Trades Division, Service Industries, Enterprise Statistics, Industrial Organization and Finance, and Agriculture (N=5)
- Field 6—Informatics and Methodology: Business Register, Tax Data, Business Survey Methods Divisions, Small Area and Administrative Data (N=4)
- Field 8—Social, Institutions and Labour Statistics: Labour Statistics (N=1)

We conducted work in three non-subject-matter divisions providing services on a corporate basis—Administrative Support Services, Informatics Technology Services and Data Access and Control Services. For example, drivers to transport tax data, provision of sanitization software, and services in the legislative context of communicating tax data to others.

We created a list of users based on those accessing files controlled by Tax Data Division information and supplemented it with additional information obtained from each of the subject-matter divisions so that we created a comprehensive list of tax data users. This list was used to identify 332 offices that we inspected in 8 of the 12 divisions in November 2004. We inspected in Industrial Organization and Finance in May as part of our pilot work, and did not inspect in Tax Data Division, Business Register or Small Area and Administrative data given their extra perimeter security.

Appendix B—Management Action Plan

Recommendation	Management Action Plan	Responsible for Action	Estimated Completion Date	Status
Tax Data Division consults with Administrative Support Services Division (service provider for drivers) to explore options for direct transport and find ways to improve packaging and include these in its procedures manual. The procedures manual should include a process to identify and log any incidents related to packaging or transport, and report them to divisional management so that appropriate action can be taken. This will provide procedures tailored for these circumstances.	Tax Data Division will arrange with ASSD to implement direct runs for STC drivers between CRA and STC sites, either as dedicated runs or as the last leg of multiple stop runs in the case of pick-ups, or the first leg in the case of deliveries. In addition, ASSD will ensure that any tax data picked up at CRA or returned to CRA are kept in a locked container during these runs. We will also make arrangements with CRA that all pick up and deliveries are made exclusively by STC drivers, discontinuing the use by CRA of commercial courier services to send tax data to STC. Finally, TDD and ASSD will implement a process to ensure any packaging and transportation anomalies that may occur are documented and brought to the attention of both directors for action as appropriate.	TDD	Sep 2005	

Recommendation	Management Action Plan	Responsible for Action	Estimated Completion Date	Status
Tax Data Division works to revise the MOU so that what is expected when Statistics Canada drivers transmit tax data is clarified.	In light of the arrangements that will be made as a result of recommendation 1, there is no need to revise the MOU as Statistics Canada will assume sole responsibility for transportation of tax data to and from CRA sites, thereby implementing more stringent security procedures than what is called for in the MOU.	TDD	Sep 2005	
Informatics Technology Services Division keep the most recent version of the sanitization software package available on its website and notify Field IT Service Managers so that they take steps to ensure that employees reporting to them sanitize computer hard drives leaving Statistics Canada using the latest version; and that ITSD also notify the Supervisor Assets Management / Quality Control in Administrative Support Services Division.	Check the software provider's web site quarterly to get the latest version when posted and carry out notification as recommended	ITSD	ongoing	DSX version 1.4 was made available in Dec 2004 and as of April 2005, is still the current version