Audit of Personnel Screening

REPORT

Audit and Evaluation Division
July 2003

Statistics Canada Statistique Canada

Canada

Table of Contents

Auditor's Statement **1**

I. Introduction **2**
Background 2
Objective 2
Scope 2
Criteria 3

II. Methodology **4**

III. Findings and Recommendations **5**
Assessing the extent of compliance 5
Improving processing 7
Recommendations 8

IV. Conclusion **8**

Appendix A—Management Action Plan **A1**

Auditor's Statement

I have completed the Audit of Personnel Screening, the objective of which was to examine the compliance with Statistics Canada *Security Practices Manual* standards on personnel screening and a related standard on access to network A at Statistics Canada—in other words, 'logical' access control pertaining to information technology security. The audit was to also identify reasons for any non-compliance in order to improve procedures.

This internal audit was carried out in accordance with the Internal Auditing Standards for the Government of Canada. During the audit period, the audit team examined security records for 493 cases and records related to 'logical' access control for 35% of these.

For indeterminate employees, there is general compliance with Chapter Three of the Statistics Canada *Security Practices Manual* requiring that the security check be completed before starting work. For determinate employees and interviewers—who may be appointed before having an enhanced reliability check if there is operational need, and students—who may be appointed prior to a check being conducted, we conclude that there is compliance, although this process could be handled in a more timely way. For deemed employees examined, we were unable to determine compliance due to methodological considerations. Access to computer system accounts is in accordance with the standard relating to access to network A (on 'logical' access control for standard computer accounts in the *Security Practices Manual*, Chapter Five.)

These conclusions are based on the assessment of findings against pre-established criteria and agreed to by the Internal Audit Committee in November 2002 and reflect the audit work conducted principally between March and June 2003.

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

December, 2003

I. Introduction

Background

Managing security in Statistics Canada—and the federal government—encompasses three main areas: physical and electronic security of information, security of assets and personnel security. The area of personnel security is essentially the proper security screening of employees up to a level of security that is commensurate with the security classification of the information required for their work.

The area of personnel security has recently gained considerable prominence on the world stage and is considered a pillar in support of both information and asset security. The impact on our reputation of either not or inappropriately screening employees could be in the extreme very damaging as in the case of a serious security breach involving an 'unscreened' employee. Recent and rapid growth in the number of employees at Statistics Canada as well as the sensitive information gathered by the Bureau, provided impetus for the audit, given an assessment that the risks are real and the potential impact very high on our reputation.

Objective

The objective of the audit was to examine the compliance with Statistics Canada *Security Practices Manual* standards on personnel screening and a related standard on 'logical' access control pertaining to information technology security. The audit was to also identify reasons for any non-compliance in order to improve procedures.

Scope

The audit focussed on the standards on personnel screening that are applied to employees, interviewers and Statistics Canada deemed employees, for example: on-site researchers, provincial officers, other federal public servants and participants in interchanges.

At the outset, contractors were defined within scope. Later, we excluded them for the following reasons:

- recent positive results of the internal audit of contracting services
- our assessment that their security risk is low
- respondent burden on Materiel and Contract Services employees

We concluded that provincial officials, other federal public servants and volunteers were low risk and low volume and did not examine their records.

Although it was within scope to look at how managers control access to designated physical information when a security clearance is in the process of being completed, we excluded this element for the following reasons:

- lower risk;
- measurement difficulties;
- timeliness concerns.

Criteria

We expected to find that:

- Employees are screened and security cleared according to the *Security Practices Manual*, Chapter Three, given the information and assets to which they have access.

Type	Chapter Three—key elements
indeterminate employees	Appointment to an indeterminate position may only be made once the enhanced reliability status has been granted.
term employees	Term employees of less than 6 months may be appointed prior to the enhanced reliability check being completed for reasons of operational necessity, as deemed required by the manager. As an essential pre-requisite, the personal references must be verified and the results must be favourable. Term appointments must not extend beyond the original term, without the incumbent having been granted the Enhanced Reliability status.
students	Appointment to student positions may be made prior to the enhanced reliability check being conducted. The check is to be initiated immediately after a decision to hire has been made. When possible, references should be verified prior to appointment, and the results favourable.
interviewers	Given the sensitivity of the function, interviewers should normally have the enhanced reliability status before they are actually engaged in collecting data. However, appointments to interviewer positions may be made prior to the enhanced reliability status being granted, in cases of operational necessity, as deemed necessary by the manager. The enhanced reliability check is to be initiated immediately after a decision to hire has been made and appointment should be delayed until the personal references are fully verified and the results favourable.

We expected to find that:

- Access to computer system accounts and to designated physical information when a security clearance is in the process of being completed is in accordance with the *Security Practices Manual*, Chapter Five.

Deemed employees are regarded as employees for the purpose of the *Statistics Act*. The Statistics Canada *Policy on Deemed Employees*, July 2002 provided additional guidance.

Personnel screening process for new hires

Personnel screening for an enhanced reliability status involves several steps, documented on the personnel screening, consent and authorization form:

- obtaining an applicant's consent to be screened and declaration concerning a criminal record;
- verifying date of birth, address, education, professional qualifications, employment history and personal character references;
- having a criminal record name check performed by the RCMP;
- if necessary, obtaining fingerprints so the RCMP can do a fingerprint check;
- receiving results; and
- making a decision.

Network access is given once the departmental security office has signed on the application form.

II. Methodology

With the assistance of a methodologist, the audit team:

- Identified new employees requiring personnel screening using the Survey Operations Pay System (SOPS) database to identify interviewers and Global, another human resources database, to identify other employees. The Global list covered the period February 1, 2002 to January 31, 2003 while the SOPS list covered a period slightly earlier—December 1, 2001 to November 30, 2002.

- Drew representative samples, checked the required information in departmental security office files and then files in Informatics Technology Services Division (ITSD) to determine when employees had been given network ID accounts. We examined departmental security office records for 493 cases and ITSD records for 35% of these. For those ITSD records possessing both dates, we verified that the departmental security office had signed the form on or before the day that ITSD gave access.

- Identified positions requiring clearance at the secret level and employees occupying them as well as cases where enhanced reliability statuses needed updating because they were older than ten years, using 'on strength' employees as of May 31, 2003 in Global.

- For deemed employees, examined 78 cases in the Research Data Centre Program database.

- Held interviews with staff in the departmental security office, Human Resources Operations Division, Regional Operations Branch, including Management, Services & Informatics managers and employees in regional offices, Informatics Technology Services Division, and the manager of the Research Data Centre Program.

III. Findings and Recommendations

Key results

- General compliance with personnel screening requirements in the *Security Practices Manual*, Chapter Three, although for term employees, interviewers and students, this process could be handled in a more timely way.
- Informatics and Technology Services Division does not issue Network User ID without approval from the security office.

Details
Assessing the extent of compliance

All employees and deemed employees at Statistics Canada require an enhanced reliability status. A minority—including those in the executive category—require a secret clearance.

For employees

New hires

For indeterminate employees, results show general compliance with the internal *Security Practices Manual* requirement that no indeterminate employee is to start work without an enhanced reliability status. Nearly 90%[1] met this criterion and 95% received this status two weeks after starting work.

Standards are less stringent and more varied for other employees, as described earlier. In cases of operational necessity, determinate employees and interviewers may start work before a clearance is completed. Less than half of determinate and student employees had their personnel screening completed when they start work, although 86%[2] and 92%[3] respectively, had it within two weeks. For interviewers, 50%[4] had their screening completed by the time they start work. Within 2 weeks, this proportion was 89%[5]. In

[1] 95% confidence interval is + or – 15%. The coefficient of variation is 9%.
[2] 95% confidence interval is + or – 12%. The coefficient of variation is 8%.
[3] 95% confidence interval is + or – 19%. The coefficient of variation is 11%.
[4] 95% confidence interval is + or – 5%. The coefficient of variation is 5%.
[5] 95% confidence interval is + or – 3%. The coefficient of variation is 2%.

Sturgeon Falls, we found complete compliance by the start date in the interviewer sample.

This audit focussed on internal standards, in place since 1991. However, the most recent *Government Security Policy*, revised effective February 1, 2002, states that "departments must ensure that, prior to the commencement of duties, individuals who require: a) access to government assets (including information) undergo a reliability check and are granted a reliability status." The Agency needs to revise its standards accordingly.

Updating employees' enhanced reliability statuses
Enhanced reliability statuses are valid for 10 years by which time they are to be updated. Results based on Global show that 11% of the 6352 employees on strength on May 31, 2003 have expired security statuses. In May 2003, the departmental security office undertook to identify expired cases and request updates. Eliminating this backlog and establishing an updating process before expiry would address the matter.

Checking expiry dates when staffing actions occur and initiating an update if necessary would offer another control. At present, we found that of the 705 expired cases, 45% had had a staffing action after the expiry date.

Secret clearances and their updates
Results from Global show that generally, employees who require a secret clearance possess one. There were a few exceptions—5 out of 193 positions classified as secret had employees occupying them without the required clearance. Action has already been taken to correct this.

Network User ID an effective control
Audit results show that Informatics and Technology Services Division does not issue Network User ID without approval from the security office.

For deemed employees

The *Statistics Act* allows for persons other than employees to provide services to carry out work as deemed employees. They can be other federal public servants, provincial officials, contractors, temporary help, Canadian and international exchange personnel, unpaid students and volunteers and those carrying out approved research projects.

Directors are accountable for ensuring that appropriate procedures are followed, including the enhanced reliability check, before providing access to sensitive statistical information for deemed employees in their divisions. The manager for the Research Data Centre Program (RDC) has similar responsibilities for RDC researchers. Responsibility rests, therefore, with many people.

Research Data Centre Program researchers
A database exists in which to record information about researchers and their projects, including the security clearance date, entered by non-security staff. There is no operational need to record the date on which researchers start to access confidential information in a Research Data Centre Program (RDC) and against which an audit might compare the date a clearance was authorized. We were unable to determine compliance because the methodology used would need to be modified significantly in order to draw a conclusion.

Improving processing

This summarizes key best practices. Managers have been provided with more detailed information.

A partnership approach
Personnel screening involves many players—managers, human resources specialists and security specialists. Developing closer working relationships to complement each other while at the same time understanding roles and responsibilities would contribute to an integrated effort and better the result.

Signing early
Having applicants sign the consent and authorization form early in the hiring process such as when invited for a written exam or interview would position managers well for compliance. Following standard written procedures incorporating this into the hiring process and shared by all staffing teams—both managers and human resources professionals—would increase the likelihood that individuals would have their clearance when they start work.

Better case management and documentation
More effective monitoring of the security office pending file for fingerprint cases would reduce its size and eliminate cases pending for long periods. Good management practice suggests that the security office has a responsibility here and there is an opportunity for it to take a leadership role, helping managers to do so as well. Well-completed consent and authorization forms facilitate later steps in the screening process, including better record-keeping and filing.

Recommendations

1. Data Access and Control Services Division revise Chapter 3 of the Statistics Canada *Security Practices Manual* in line with the revised *Government Security Policy* for approval by Policy Committee and widely communicate changes. A key item will be the review of the timing expected for reliability statuses with a view to improving current practices.

2. Data Access and Control Services Division, Human Resources Operations Division and Regional Operations Branch partner to improve the monitoring and management of personnel screening, periodically reporting results to the Confidentiality and Legislation Committee.

3. Security status and expiry information about employees and deemed employees be entered into the relevant corporate database by security staff only, following the best practice in place for the Global database. The databases to which this practice should be extended are: Survey Operations Pay System for interviewers; and the RDC Project Management System Database, maintained under the direction of the Manager of the Research Data Centre Program and to include all deemed-employee researchers.

IV. Conclusion

For indeterminate employees, there is general compliance with Chapter Three of the Statistics Canada *Security Practices Manual* requiring that the security check be completed before starting work. For determinate employees and interviewers—who may be appointed before having an enhanced reliability check if there is operational need, and students—who may be appointed prior to a check being conducted, we conclude that there is compliance, although this process could be handled in a more timely way. For deemed employees examined, we were unable to determine compliance due to methodological considerations. Access to computer system accounts is in accordance with the standard relating to access to network A (on 'logical' access control for standard computer accounts in the *Security Practices Manual*, Chapter Five.)

Appendix A—Management Action Plan

Recommendations	Management Action Plan	Responsible for Action	Estimated Completion Date	Status
1. Data Access and Control Services Division revise Chapter 3 of the Statistics Canada *Security Practices Manual* in line with the revised *Government Security Policy* for approval by Policy Committee and widely communicate changes. A key item will be the review of the timing expected for reliability statuses with a view to improving current practices.	DACS has met with HR and received input from the Regional Offices regarding the changes that need to be made to the Screening Policy.	DACS/HR	October 2003	Completed
	HR is conducting an in-depth analysis of the hiring steps and will endeavour to build into the re-engineered hiring steps the requirement for the security screening of all indeterminate, term, casual and students to be completed prior to employment.	HR	November 2003	On-going
	Communication with senior managers, HR professionals, administrative community and DACS Security will be required so that the necessary changes are successfully implemented.	HR/DACS	May 2004	Planning of communication strategy: January 2004
	Discussion will need to occur with 2006 Census team regarding the security clearance requirements for the 2006 Census enumerators.	HR/DACS/Census	May 2004	Already initiated
	DACS will propose the changes that need to be made to the *Security Practices Manual.*	DACS	May 2004	Already initiated

Recommendations	Management Action Plan	Responsible for Action	Estimated Completion Date	Status
2. Data Access and Control Services Division, Human Resources Operations Division and Regional Operations Branch partner to improve the monitoring and management of personnel screening, periodically reporting results to the Confidentiality and Legislation Committee.	Eliminating expired status in GLOBAL system	DACS security	November 2003	Backlog was completed by November 2003. Review on a monthly basis and all soon-to-be expired clearances actioned 2 months prior to expiry date.
	Eliminating expired status in SOPS	DACS/ROB	August 2004	Work to eliminate backlog to commence in March 2004. Review on a monthly basis and all soon-to-be expired clearances actioned 2 months prior to expiry date.
	Best practices	HR/DACS/ROB	On-going	On-going
	Improving management through future administrative systems re-engineering projects	HR/DACS	2005	HR/DACS identified needs and communicated them to re-engineering project team. (These are being incorporated into the administrative community SSI proposal.)

Recommendations	Management Action Plan	Responsible for Action	Estimated Completion Date	Status
	Monitoring compliance	DACS	On-going	Weekly updates being given and monthly reports starting Oct 2003 Report to appropriate committee on an annual basis
3. Security status and expiry information about employees and deemed employees be entered into the relevant corporate database by security staff only, following the best practice in place for the Global database. The databases to which this practice should be extended are: Survey Operations Pay System for interviewers; and the RDC Project Management System Database, maintained under the direction of the Manager of the Research Data Centre Program and to include all deemed-employee researchers.	SOPS RDC Project Management System Database	ROB/DACS RDC/DACS	August 2004 To be determined	DACS access to SOPS by March 2004 to begin entering new data and bringing SOPS up-to-date with security information Discussion underway with RDC manager