Security Audit Follow-up Report

April 2003

Audit and Evaluation Branch

Environment Canada Environnement Canada

Canada

Report Clearance Steps

Follow-up process implemented	November 2002
Report completed	March 2003
Factual Review	April 2003
Report approved by Departmental Audit and Evaluation Committee (DAEC)	January 8, 2004

Acronyms used in the report

ADM	Assistant Deputy Minister
BL	Business Line
CLC	Canadian Labour Code
CMC	Canadian Meteorological Centre
DAEC	Departmental Audit and Evaluation Committee
DG	Director General
DSO	Department Security Officer
EC	Environment Canada
EMB	Environment Management Board (Current name: Executive Committee)
ERC	Environment Resource Committee
GSP	Government Security Policy
HR	Human Resources
IT	Information Technology
NHQ	National Head Quarters
OS	Operating System
OSH	Occupational Safety and Health
OH&S	Occupational Health and Safety (current name)
PCO	Privy Council Office
TRA	Threat and Risk Assessment

Acknowledgments

This Follow-up was completed by Hallux Inc. under contract with the direction of S. Debidin. We would like to thank all those who contributed to this project.

Table of Contents

Executive Summary

This follow-up audit was conducted to assess steps taken to-date in response to the five recommendations made in the Security Audit Report of August 2000, to identify measures implemented with respect to the additional funding and to assess the level of residual risk.

Since that time two events have impacted the security community at Environment Canada (EC). First, the tragic events of September 11, 2001 ("9-11") brought the issue of security management home to every Canadian. The Privy Council Office (PCO) issued a memo to all Departmental Security Officers (DSO) requesting that the level of security at government facilities be increased to a “heightened state of security”. Second, the revision of the Government Security Policy (GSP) - issued in February 2002 - reflected necessary security enhancements as a result of "9-11" and placed more emphasis on departments for improved security administration.

The follow-up audit report focuses on progress made with regards to the five recommendations of the Security Audit. Environment Canada has moved, like other federal departments, to address the requirements for improved baseline physical security, consistent with PCO direction and GSP revisions. The Department's decision to fund the development of a national security organization is a critical step forward in addressing the strategic nature of security risk, even more so at this time when global security concerns continue to impact government operations. The follow-up also recognizes that, post- "9-11", communication and cooperation among EC's security community within it's regions, National Headquarters (NHQ) and service areas (i.e. Environment Protection Services, Environment Conservation Services and Meteorological Services of Canada) have increased while also building expectations for improved management practices.

The Department's security community has undertaken the challenge of its task on a best efforts basis to date. Senior management's attention will now be needed to address the three recommendations from the Security Audit of 2000, where effective action is still pending. The following are the main results emanating from this follow-up audit:

a) *It would be beneficial to the Department if the scope and authority for the Departmental Security Officer in security management and the underlying security management framework are clarified within the EC context, in order to support the required security program. Such clarification is also needed in order to ensure that benefits resulting from the Department's now significant investment proposition to develop a national security organization are adequately monitored and reported.*

b) *A mandatory department-wide security awareness program that informs and regularly reminds all departmental personnel of security responsibilities, issues and concerns, as well as providing for up to date training for individuals with security responsibilities, is needed in order to ensure that departmental personnel respond appropriately in security threat circumstances.*

c) *The absence of a department-wide Business Continuity Planning program under the coordinating authority of the DSO poses some risk that the delivery of departmental services may be compromised in the event of a disaster.*

d) A risk management framework incorporating a formal, department-wide methodology for addressing security risk management on an on-going basis is needed to ensure the Department is prepared to manage changes in a threat environment.

e) Considering the Department's increased investment in a national security organization and security program implementation, regular progress reporting by the DSO to the Management, Resources and Results Committee and the Executive Committee (as required) is needed.

Security Program Managers have agreed to the findings of this Audit Follow-up Report.

I. Introduction

1.0 Background

Departments are accountable for the implementation of the Government Security Policy (GSP) and Operational Standards (OS) and must conduct internal audits to ensure compliance with the policy and its effectiveness and efficiency at least once every five years starting in 1994. In February 2002, the Treasury Board issued a revised GSP, and is in the process of updating the supporting operational standards.

The September 11, 2001 ("9-11"), terrorist attacks in the United States precipitated a memo from the Privy Council Office (PCO) to all Departmental Security Officers requesting that the level of security at government facilities be increased to a "heightened state of security". As a result, security managers were requested to examine their organizations' readiness to respond to security emergencies. Environmental Management Board members at a post-September 11 meeting also raised concerns regarding the department's ability and readiness to respond to emergencies.

Despite a request from the Department for resources to assist with security enhancement initiatives, no additional resources were forthcoming and Environment Canada (EC) was directed to absorb the costs within its existing budget.

In Fiscal Year (FY) 2001/2002, the Environment Resource Committee (ERC) allocated $475K to assist with immediate funding pressures resulting from the requirements for heightened security measures. In July 2002, the ERC approved $1.0 M for FY 2002/2003. Furthermore, in light of the fact that funding pressures for enhanced security measures are expected to continue, the department is currently developing a business case to address funding requirements on an ongoing basis, i.e., to implement Threat and Risk Assessment (TRA) recommendations and maintain a viable security community in Environment Canada.

Security is often described as the protection of sensitive information, material assets and people from threats using safeguards designed to ensure their *confidentiality, integrity*, *availability* and *well-being.* The revised GSP describes a departmental security program model as having the following components:

i) organizational structure,
ii) administrative procedures, and
iii) several sub-systems including:
    a) physical security,
    b) information technology security
    c) personnel security,
    d) security and contingency management,
    e) security and contracting management,
    f) protection of employees,
    g) security outside Canada,
    h) identification of assets,
    i) security training, awareness and briefings, and
    j) security in emergency and increased threat situations.

The efficiency and effectiveness of a security program depend upon these elements performing independently and in combination. Where responsibility for the various elements may be decentralized or assigned to different organizational units, a coordinated approach to planning, management and administration of the security program as a whole is critical.

In August 2000, Hallux Consulting Inc completed an audit of Security of EC. The audit made several observations and provided five (5) recommendations. Following a review of the recommendations, management agreed to implement all the recommendations.

2.0 Objectives and Scope

The overall objective of this follow-up audit was to assess progress in implementing the five recommendations made in the Audit Report of 2000. In addition the follow-up was tasked to identify measures implemented with respect to additional funding allocated and assess the level of residual exposure.

The scope of this follow-up did not include Information Technology (IT) Security and specific Occupational Health and Safety (OH&S) issues as each area has been (or will be) addressed by a separate review.

3.0 Audit Approach

The follow-up audit assignment followed a similar methodology and approach as the one used in the original audit, based on the Treasury Board of Canada Secretariat's (TBS) audit guidelines for security. As the assignment was not a complete audit but a follow-up to a previously completed audit, only a select number of individuals were interviewed. In total 13 individuals participated, reflecting headquarters, regional offices and program area responsibilities. Documentation gathered during the follow-up audit was reviewed and reflected in the analysis.

The audit follow-up assignment commenced on November 6, 2002, and the conduct phase ended on January 17, 2003. The audit team expresses its gratitude for the contribution of the personnel who participated in the audit.

II. Findings and Management Response

4.0 Security Organization and Administration

Security Audit 2000 Recommendation #1: It is recommended that a senior level position with DSO responsibility, reporting to the DG Administration and accountable for the implementation of a security program, be established in order to strengthen the organization and administration of department-wide security at EC.

Management Response (May 2001)

A new Departmental Security Officer (DSO) was appointed and reports directly to the Director General (DG), Administration. The DG, Administration continues to represent the deputy head in dealings with the Treasury Board.

In order to ensure accountability and strengthen the organization and administration of the Department-wide security program, a decision was made to reintegrate the Departmental security staff of EC under the responsibility of the Director, Real Property & Security. The transition was completed April 1, 2001.

Audit Follow-up Finding (March 2003)

4.1 DSO Role

The intent of the recommendation in the Security Audit of 2000 was clearly to provide for an increased departmental capability to effectively plan for a coordinated response and mitigation to critical security events. While some coordinative elements of department-wide security have been addressed as a consequence of the aftermath of "9-11", the scope and authority for Departmental Security Officer responsibility requires clarification, so as to reduce the risk associated with managing a potential security threat situation.

The DSO has been formally appointed, as required by the Government Security Policy. As a follow-up to the recommendation of the previous audit, the Deputy Minister confirmed the appointment of the Director, National Operations in the function of the Departmental Security Officer, by way of a memorandum signed on February 14, 2001.

The GSP also recommends that the DSO have sufficient security experience and be strategically positioned within the organization in order to accomplish the role effectively. Within EC, the DSO reports directly to the Director General, Administration who, in turn, represents the Deputy Head in dealings with the TBS.

It is a requirement of the Security Policy that the DSO establish and direct a security program that ensures co-ordination of all policy functions and implementation of policy requirements. Formal documentation, such as a job description or terms of reference, would be helpful in defining the scope of the DSO role and enhancing clarity in the overall accountability of the DSO.

For example, while the Director, National Operations is EC's DSO, departmental security is operationally led by the Director, Real Property and Security through a small staff of security officers. Both positions report to the DG, Administration. For some months now the Director, National Operations - the DSO - has also been the acting Director General, Administration and the position of the Director, National Operations has not been backfilled.

EC's Security staff reference the GSP as a general outline for DSO responsibility, yet in key issues of departmental security the EC-DSO's authority does not appear to be adequately defined. For example, a formal linkage to IT Security is absent, EC's Crisis Management Structure has not been formalized and proposed roles and responsibilities for the investigation of incidents remain to be implemented.

4.2 Security Management Framework

Two highly positive outcomes have occurred in the Department's security community, since the Security Audit of 2000, that go a long way to strengthening the Department's security administration.

First, since "9-11" a significant degree of engagement has been reported within the EC security community as part of the Department's internal security response. In particular, individuals interviewed agreed that communication within the security community had improved greatly, largely due to the coordinative influence of permanently staffing the Chief, Security position at National Head Quarters (NHQ). As a result, bi-weekly teleconference meetings have occurred regularly, thereby providing a forum for consultation and participation on updated security procedures, including the EC Suspect Package guidelines and EC Emergency Preparedness procedures.

Second, coordination has been facilitated by withdrawal from a local shared security services agreement with Indian and Northern Affairs Canada. Repatriation of security responsibilities within the Real Property and Security Division has resulted in improvements in passport processing and personnel security clearances. For example, employees wishing to travel internationally on government passports and visas (rather than personal passports) have increased the demand for passport processing by 60% since "9-11".

In other key areas, the Department's security management framework requires more attention (in particular, planning, organizing, implementing and monitoring) in order to facilitate a more effective departmental security program that allows the Department to adequately protect its employees, assets and service delivery.

Planning has been hampered by the lack of an overarching governance framework for corporate security. The security group has attempted to address security issues on a best-efforts basis, tapping into a relatively stable pool of resources within the Department's deployed security community and the experience of senior staff at NHQ. A business case approach has been utilized to document and justify the on-going importance of the security function at Environment Canada and to formulate priorities for security program planning and implementation. Environment Canada's Security Policy, for example, has not yet been fully updated, pending the issuance of revised TBS Operational Standards that underlie the updated GSP. That being said, it must be noted that the EC security community has expended much effort since "9-11" on the development of key security procedures, as mentioned below. Furthermore, critical functions, such as Business Continuity Planning

(BCP) or Business Resumption Planning (BRP) have not yet been staffed for leadership, even though an initiative is in place to evaluate the gap between GSP requirements and the department's current BCP posture. It is noted, however, that the staffing of the BCP position has been addressed in the business case.

The evolving Security Business Case attempts to address security gaps brought to light by the "September 11" response and tackle the impact of the revised Government Security Policy on the administration of departmental security. In addition, the Business Case proposes concomitant funding options, already approved at the Management, Administration, and Policy Table.

Environment Canada's matrix management approach[1] encourages a high degree of consultation and collaboration to ensure the success of all departmental programs. In the long-term such collaboration will inevitably serve to strengthen the Department's security program. In the short-term, however, the Department may not be able to generate an adequate unified response to deploy effective security countermeasures in an increased threat situation. The absence of a department-wide Business Continuity Planning program, as noted later in this report, illustrates the exposure.

In addition, the security function does not, at this time, have a capability to investigate and report on security incidents that may indicate department-wide vulnerabilities. For example, in recent months there have been two separate incidents involving the theft of firearms from departmental premises. Both incidents were as a result of break and entry offences, one in Moncton and one in North Vancouver. There are several departmental sites where firearms are purchased, maintained and stored. The Enforcement Branches of Environmental Conservation Services (ECS) and Environmental Protection Services (EPS) as well as the Meteorological Service of Canada, utilize departmental firearms (rifles, shotguns and handguns) to protect EC employees from animal attacks in the wild, to collect wildlife species for study, to terminate seriously wounded or dangerous animals and to effect arrests on individuals in violation of the law.

In the above-noted incidents, the thieves also stole ammunition, defensive equipment, computers, a vehicle and other valuable material. While both matters are under investigation by the police, there is some concern that the theft of a firearm and ammunition may have posed a hazardous occurrence for some employees possibly on the premises during one of the incidents. According to the GSP, departments must develop procedures for reporting and investigating security incidents and taking corrective action. The current procedure within EC is for all regions and services to submit their incident reports to HQ for review and annual reporting, including reporting losses in the public accounts. At this time, the Department does not have a central database listing security incidents and this could compromise its ability to evaluate possible trends and take mitigating actions. In addition, the Department does not possess an effective internal investigative capability across all regions for it to conduct an appropriate in-depth investigation of causal factors. Taken together, these shortcomings may reduce EC’s capacity to effectively address future occurrences.

[1] A detailed description of the matrix management approach at Environment Canada is provided in the Accountabilities Charter in Appendix A.

The security function has, however, begun the process of establishing "designated security officer" (DESO) positions in regional and program areas. Funding arrangements are being developed to ensure that these are on-going, full-time positions dedicated to achieving security objectives. The Regional Directors General (RDG) community has endorsed roles and responsibilities of the designated security officers and the NHQ security group is attempting to ensure consistency in qualifications, staffing, training and development of this cadre of staff. DESOs are proposed as regional/program resources, not deployed staff that are managed centrally.

Implementation of standardized security processes and protocols across the department is evolving. Under the proposed DESO structure, departmentally determined security objectives are expected to be consistently cascaded to Regions and Service areas since DESOs will be dedicated security resources. At present security coordinators in most regions may not have jurisdiction for all components of security, as proposed in the DESO job description. In some regions it is not uncommon for security roles to be shared out among different job functions and organizational units. In one Region, for example, one clerk spends 30% of their time on Physical Security matters, while another clerk spends 10% of their time on Personnel Security tasks. While regional security coordinators have considerable autonomy, there is an increased recognition that the security community in EC can benefit from sharing work products and building common processes.

A Security Report is tabled annually at the Environmental Management Board (EMB). Security reporting does not form part of a standing agenda at executive and most regional management board meetings on a regular (e.g. monthly) basis. Nevertheless, in the months immediately following "9-11", the Security function participated frequently at EMB meetings in order to update senior management on the response around EC's critical facilities and business priorities in the regions and service areas. This exercise included the support of regional coordinators at regional management meetings. Within EC's management arena, then, the Security function generally maintains a rather low profile. It does not seem to be engaged at the level of strategic risk management, being relied on only to react to actual security occurrences.

The GSP requirement for the DSO to establish and direct a department-wide security program is difficult to achieve given the present EC accountability framework. Security exists as a sub-component of the Corporate Function's Administration area. EC's accountability framework places responsibility for establishing and monitoring program priorities at the business lines (BL) level, with implementation and integration at the Regional Director General (RDG) level. It is the RDGs who are responsible for ensuring that the functional objectives of a departmental security program are achieved through regional prioritization and resources. As a result, the DSO is effectively limited in exercising significant authority over the scope of security (i.e. GSP) functions within the Department.

The audit follow-up concludes that management actions to date have not fully addressed the 2000 Security Audit's recommendation.

4.3 Audit follow-up recommendation

There is no recommendation associated with this element of the follow-up audit, however, it is suggested that senior management clarify the authority and scope of the role of the Departmental Security Officer (DSO) with respect to establishing and directing a security program that ensures co-ordination of all Security policy functions.

4.4 Management Response

Since the August 2000 Security Audit, the department has formally appointed a Departmental Security Officer (DSO). Additionally, two highly positive outcomes have occurred in the department's security community that go a long way to strengthening the administration of the security program. These outcomes include a significant degree of increased communication and engagement within the EC security community, as well as the withdrawal from a locally shared security services agreement with Indian and Northern Affairs Canada.

Although there is no recommendation associated with this element, the department will undertake to formalize the roles and responsibilities of the DSO and incorporate same in the EC Security Policy. This will ensure the following:

- **necessary linkages with regions/services are maintained with respect to reporting of security incidents/investigations**
- **linkages to IT security are clearly defined; and**
- **the DSO acts as the single window to the DM.**

5.0 Security Awareness

Security Audit 2000 Recommendation #2: It is recommended that the DSO develops, coordinates, implements and communicates an on-going department-wide security awareness program, with particular emphasis on:

- The protection of sensitive information;
- Transmission of sensitive information by electronic means;
- Requirements for security in contracts;
- Requirements for appropriate security clearances for employees.

Management Response (May 2001)

An ongoing Security Awareness program is to be provided department-wide with the use of existing security tools and the implementation of the new security awareness initiatives. To date, the security policy and awareness team has developed a new electronic security awareness presentation which is currently being used in the National Capital Region (NCR) to brief various management tables (i.e. Canadian Environmental Assessment Agency; EPS Enforcement, etc.). The presentation will be shared with all Regional security officers at the upcoming annual workshop in the fall (October 2001).

Security Newsletters are issued on an ongoing and as required basis in the NCR and across the Department.

Audit Follow-up Finding (March 2003)

There is, as yet, no formal department-wide security awareness program in place for employees of the Department. In the National Capital Region, awareness sessions are conducted on a quarterly basis following security sweeps to all staff on the floor regarding the results of the sweep. NCR also provides quarterly bulletins to all EC employees as well as to regional security offices. Over the last three years, training sessions have been provided annually by NCR to the departmental security community by security experts including Treasury Board, the Royal Canadian Mounted Police (RCMP) and others. There are other times when Human Resource (HR) provides Employee Orientation Package as general information in addition to information available on the EC website. Because of the administrative structure of the department, implementation of security initiatives including training is the responsibility of the regions. Therefore, the lack of a requirement for specific up-to-date training for security staff across all regions increases the risk that departmental personnel might fail to respond appropriately in security threat circumstances.

On-going efforts have been made to introduce components of a security awareness program aimed at some operational and administrative staff. A bi-weekly teleconference, for example, provides regular communication among the Department's security community. Furthermore, the NHQ security group, in concert with regional coordinators has generated and published procedures to address certain physical security concerns as a result of "9-11". These include the Suspect Package Guidelines, Emergency Preparedness procedures, Departmental Travel Directives, and others. In addition, IT staff offer IT Security orientation to employees on subjects like system access, data transmission and download of electronic information.

At a departmental level, a formal security awareness program to regularly inform and remind EC employees of security concerns and issues is not in place. For example, there is no security-centred orientation package that informs employees about their responsibility regarding security on a regular basis beside quarterly briefed following a sweep. On a day-to-day basis reliance is placed on ad hoc processes to inform or update employees and management teams.

Security is not generally an agenda item at management meetings, as noted earlier, unless reporting is required in reaction to specific incidents. As an illustration, the two previously mentioned break and entry occurrences at EC sites on the Atlantic and Pacific coasts that resulted in firearms being stolen, did focus attention, as departmental procedures are now being considered to supplement existing legislative requirements and EPS procedures for the security of firearms and ammunition. Individuals interviewed portray the culture of the Department as being reactive, whereby security comprises an administrative process rather than a risk mitigation strategy.

Under the Department's management framework, Regions and Service areas are responsible for their respective staff. Therefore, the method of delivering security awareness and the scope of the message is delegated to the local manager. Security coordinators are required to make use of available tools to promote security awareness. Some local security coordinators, however, do not have the time or resources to undertake security awareness initiatives. Due to the workload generated, these security coordinators only pass on enough information that the coordinator believes to be relevant. In one Region,

the security coordinator had developed a presentation on personnel screening to inform the regional management team, but had not had the opportunity or resources to undertake the presentation. In the absence of a formal national security awareness program, security staff point employees and managers to information in existing repositories, where available, such as the National Capital Region's website on Infolane, or a regional intranet website used for posting security information.

Standardized security training for departmental security personnel is not in place although the proposed DESO initiative is expected to include specific DESO Security training. A course outline has been developed and the training will form part of the security workshop in May or June 2003, subject to completion of DESO staffing. At the time of the audit follow-up, however, there was no formal security training plan in place for existing security coordinators. Since most security coordinators have been performing the security coordination role for several years, there is little interest in formal training. Presently, training is not a formal performance objective for current security coordinator positions.

The audit follow-up concludes that management actions to date related to this recommendation of the Security Audit have not been sufficient to mitigate the risk and address the requirements of the GSP.

5.1 Audit follow-up recommendation 1

It is recommended that, included with the security function's objectives for 2003-04 and on, the DSO must develop, implement and maintain a department-wide security awareness and training program that:

a) informs and regularly reminds all departmental personnel of security responsibilities, issues and concerns; and
b) provides appropriate up to date training for individuals with security responsibilities.

5.2 Management Response

Prior to "9-11", the security program was being managed with limited HR resources. In the regions, a designated security position did not exist and these functions were carried out by the Administrative staff who were also responsible for many other tasks. Following the events of September 11, the department put forward a funding request to enhance capacity in headquarters and in the regions/services. The business case was approved by ERC in May 2003 and staffing is currently underway in all regions and at the national level to ensure appropriate HR resources are in place to implement a department-wide security awareness program including:

- **staffing of Designated Security Officer positions in the regions/services**
- **staffing of National Security Office positions (Chief; Passport Officer; BCP Coordinator; and a Threat and Risk Assessment/Ministerial Events Coordinator).**

In addition, the department has committed to developing a department-wide security awareness program by implementing the following:

- **regions/service to develop annual workplans including:**
  - **provision of regular training to regional/service employees**

- **conduct of security sweeps (protection of sensitive information)**
- **issuance of orientation package for new employees**
- **annual training plans for security personnel**
- **quarterly reporting to the DSO**

- **the National Security Office will undertake the following:**
  - **continue to coordinate annual workshops/training sessions, quarterly bulletins, and the development of tools (policies; directives; orientation package, presentation material, etc.)**
  - **develop and implement a security awareness program across the department**
  - **develop departmental workplans and provide annual report to the Deputy Minister (DM); and**
  - **ensure the provision of regular (quarterly) progress reports to Management, Resources and Results Committee on the status of ongoing security program implementation.**

6.0 Risk Management

Security Audit 2000 Recommendation #3: It is recommended that the DSO institute a department-wide process for Threat and Risk Assessments that include documented procedures for conducting TRAs, reporting their results and monitoring any follow-up actions.

Management Response (May 2001)

The Security Division will resume its efforts relating to the conduct of a Departmental TRA building on the audit recommendations. A department-wide risk management framework will be implemented, including:

a) development of an electronic incident reporting system;
b) development of a losses of money program;
c) development and implementation of an annual TRA work plan; and
d) establishment of a central repository for TRA reports.

Audit Follow-up Finding (March 2003)

Some progress in undertaking Threat and Risk Assessments has been made. Nevertheless, a formal, department-wide methodology for addressing security risk management on an on-going basis is lacking. As a result there is a risk that the Department may be ill-prepared to manage changes in the threat environment.

Clearly the events of "Sept 11" elevated the profile of security around the world, in the nation and within the Department. At EC, Security was discussed at management tables and security initiatives were reported to management teams. As a result some changes to department security came about, including enhanced reliability clearance for all staff, increased physical security measures such as wearing of ID cards, card access control improvements, suspicious package measures and so on. A Department-level TRA, pending since 1999, has not been performed and no TRAs have been initiated during 2002-03. It is

acknowledged though that NHQ Security had funded about 20 TRAs across the country at end of fiscal year 2001-02.

The security function has not been adequately resourced to establish a credible, ongoing process to address security risks in the Department. The post-"9-11" TRA exercise pointed to a lack of an adequate methodology for ensuring consistency and credibility in TRAs. Some TRA inspections were conducted in a few hours, with limited scope and little input from local staff. Being hurriedly executed prior to year-end, the TRAs were often seen as not affording a commonality of purpose that could provide consistent results. Consequently the security community tended to see the TRA conclusions as stating the obvious about known priorities.

Some recommendations emanating from the TRA process were implemented based on the priorities of local facility managers and available resources to institute remedial action. The following illustrates the differences in the manner in which security issues are addressed in the regions:

- In one Region 10 TRAs were performed, but funding to implement TRA recommendations has not been available;

- In another Region money was taken from other sections to implement some recommendations such as the addition of cameras and guards;

- In one Regional Office 65 recommendations ensued from one facility TRA;

- Another area generated 25 recommendations, estimated at $1M, from the site TRA, and management opted to reallocate $350K from within program areas to implement priority items.

The lack of an overall security risk management process poses a dilemma for the security community as each TRA generates recommendations that will require resources to implement. Most areas in the Department have to deal with resource constraints and the EC security community has sought to support business line managers by advocating additional funds to address known security priorities through the medium of the evolving Security Business Case. It is estimated that it will cost the Department approximately $3.5M over 7 years to address recommendations in the 2001-02 TRA exercise.

The security community is mandated to advise and assist business line managers in assessing their respective security risk. It is then up to the business line managers to implement recommendations. Some local managers will have available funds and implement priority recommendations immediately. Others will not have the resources to implement similar priorities and will need to pursue an ERC recommendation for Executive Committee funding approval. As a result, responses to TRA priorities may not be consistent across the department.

The Department has started to address the recommendation in the Security Audit Report of 2000, but the risk management framework is not yet in place to assure that the level of risk is acceptable and the balance between operational needs and security is adequate.

6.1 Audit follow-up recommendation 2

It is recommended that the DSO proceed to implement the agreed management actions by instituting a department-wide risk management framework that allows for the on-going assessment of threats and risks.

6.2 Management Response

After the events of September 11, the department initiated TRAs at major EC facilities which resulted in numerous recommendations for improving physical security such as access control. The business case requested funding up to $3.5M over 7 years to address the recommendations. The May 2003 ERC decision was to implement and fund TRA recommendations from existing regional budgets, rather than creating a central fund. Some facilities have implemented recommendations, while others are identifying funding sources to proceed with implementation.

Once staffing of the TRA/Ministerial Events Coordinator position at headquarters is actioned, the National Security Office will:

- **develop an electronic incident reporting system for monitoring and trend analysis**
- **develop an annual TRA workplan at the departmental level (with input from regions/services) to include:**
  - **a 5-year planning cycle**
  - **the conduct of a comprehensive TRA at each site every 5 years**
  - **an annual review of each site to address potential changes in the threat environment (checklist update)**
- **establish a central repository for TRA reports and monitor progress re: implementation of recommendations (to be included in annual report to Deputy Minister).**

7.0 Physical & Personnel Security

Security Audit 2000 Recommendation #4: It is recommended that the DSO facilitate the implementation of standardized level of physical access controls for key facilities (e.g. LTC, PVM and each Regional Office) and zones within each facility.

Management Response (May 2001)

The Security Division, in consultation with the national security community, will develop a standardized level of physical access controls for key facilities. This approach will apply to all new installations or system upgrades.

Audit Follow-up Finding (March 2003)

Action has been evident in improving physical and personnel security regimes within the department. On-going effort is required to ensure that gains are maintained and initiatives to standardize controls are implemented.

7.1 Physical Access Controls

The department has implemented basic physical access controls at major EC facilities, in large part as a result of PCO guidelines to all departments following "9-11". For example, employees are required to wear their ID badges at all work locations. Visitors also are generally signed in and escorted. Access control measures include card readers, the presence of security guards, or both, in larger facilities. Card access is now deemed to be a common installation for new EC locations. It is estimated that ID badges are worn by about 80% of individuals. Within smaller facilities, where staff are generally know to each other, physical access controls are more relaxed. The recent TRA exercise illustrated that a standardized level of access controls has yet to be achieved across the Department. For example, there are 9 different swipe card systems in one Region alone. In another Region card access control exists in only one out of 6 major sites. The inconsistent application of security standards among similar EC-occupied facilities is most often attributed to differing facility types (e.g. PWGSC-owned, PWGSC-leased, EC-owned, etc).

NHQ Security expect that impending revisions to the new GSP's Operational Standards will include mandatory, standardized access controls for government facilities, and once released EC will then strive to implement such standardized controls.

7.2 Personnel Screening

Security screening has been emphasized subsequent to "9-11" with an effort to update all security classifications in the Department. Security clearance requests are centrally processed through NCR Security using RCMP services. The minimum security level is now “reliability status" within the Department, applicable to all new employees. Some aberrations may still exist where, for example, an incumbent security coordinator, may not yet be upgraded from reliability status to secret clearance.

While continued effort is needed in this area, the audit follow-up concludes that the Department has embarked on a course to improve and update physical access security controls where operational requirements dictate.

7.3 Audit follow-up recommendation

There is no recommendation associated with this element of the follow-up audit. It is suggested, however, that current initiatives by NHQ Security and the security community to implement physical security improvements identified through TRAs continue to be actively pursued.

8.0 Business Continuity & Resumption Planning

Security Audit 2000 Recommendation #5: It is recommended that the DSO coordinates a central point of contact for business continuity and resumption plans and monitors the updating of plans on an annual basis.

Management Response (May 2001)

The existing Business Resumption Plans developed as part of the Y2K exercise are being maintained by the Real Property & Security Branch. A central repository of individual plans will be established. Annual call letters will be issued to regional and service contacts to ensure accuracy and integrity of information. A note will be issued to the DG of Systems and Informatics Directorate to ensure maintenance of the overall Departmental Business Continuity Plan.

Audit Follow-up Finding (March 2003)

There is, at present, no department-wide Business Continuity Planning program established under the authority of the DSO. As a consequence there is a risk that the delivery of departmental services may be compromised in the event of a disaster. Furthermore, the Department has no Crisis Management Plan at present, with a previously proposed Crisis Management Plan having been set aside by senior management.

The GSP requires that departments establish a BCP program within the context of the departmental security program and organization. This program must include a governance structure with authorities and responsibilities for the BCP program, and for the development and approval of business continuity plans.

At present the authority and responsibility for a department-wide BCP program has not been formally assigned, and there is currently no National Coordinator for a BCP program. Expertise in BCP is considered lacking within EC, with the exception of Environment Protection Service's emergency planning for environmental disasters and resident expertise in Weather Centre operations. Not only has the DSO accountability for BCP yet to be formalized within EC, the security organization has not been funded to satisfy the requirement for a BCP program. While the business case put forward by NHQ security organization has identified additional resources, NHQ security organization has indicated that steps have been initiated to staff the position.

The Treasury Board Secretariat has indicated that no incremental resources are available for BCP and resources must be found internally within the Department's A-base budget. Some regional staff indicate that BCPs may be considered a priority regionally only when the associated funding is made available. The Security function has included funding requirements for BCP in the Security Business Case as a “need to have” item.

Furthermore, it is generally accepted that departmental plans to ensure BCPs are regularly reviewed and tested are not in place. BCPs are maintained locally and most regions acknowledge that these plans have not been formally updated since the conclusion of the Year 2000 contingency. However, government wide mission critical areas such as the Weather Centre have very detailed continuity plans that, like other key sites' BCPs, are updated annually. Some added emphasis is provided at sites where workplace safety concerns predominate, such as laboratory facilities. Nevertheless, coordination at a departmental level is not present.

In recognition of the Department's exposure, the security function has commissioned a BCP gap analysis to determine the current situation and what is required to be in place under the new TBS BCP draft standard. The report will be completed by the end of March 2003.

Regional coordinators, who will assume the BCP coordination role in regions under proposed DESO roles and responsibilities, point to the need for BCP training, briefing materials and process templates to animate such an activity.

The audit follow-up concludes that management actions to date related to this recommendation of the Security Audit have not been sufficient to mitigate the risk and address the requirements of the GSP.

8.1 Audit follow-up recommendation 3

It is recommended that the DSO proceed to implement the previously agreed management actions to institute a department-wide BCP program including

a) assigning a lead role for a departmental BCP coordinator; and
b) addressing any gaps identified between the Security policy /BCP Operating Standard and current departmental posture.

8.2 Management Response

With the recently approved funding to increase HR capacity in the area of Physical Security, the following activities are currently underway:

- **staffing of a National BCP Coordinator position in concert with staffing of the regional/service Designated Security Officer positions. Once the staffing actions are complete (anticipated this Fall 2003), the department will continue to address this recommendation by:**
- **establishing a BCP program and addressing findings in the Gap Analysis completed in March 2003, including:**
  - **update of Governance Structure and Crisis Management Organization**
  - **update Business Impact Analyses at critical facilities**
  - **ensure up-to-date contingency and business resumption plans exist for critical facilities at the departmental, regional and site levels and ensure the plans are organized in a convenient format for easy access in the event of an emergency**
- **ensure BCP program readiness by:**
  - **plan validation – ongoing review and revision**
  - **training**
  - **testing**
  - **development of audit cycle.**

9.0 Funding

As part of the scope of this follow-up assignment, the funding allocated to the security community since the Security Audit of 2000 was examined in order to identify measures implemented with respect to the additional funding and assess management's investment in security initiatives.

Since the last audit, $2,475,000 has been provided or approved for the administration of departmental security for fiscal 2001-02, 2002-03 and fiscal 2003-04.

2001- 02
In the latter half of fiscal 2001-2002, the Department provided $475,000 for security within the NCR and corporate areas as a response to the September 11, 2001 events, as follows:

- $200,000 was spent for performing TRAs at 20 key facilities across the country.
- $100,000 was allocated for additional security guards to supplement security at Place Vincent Massey, and Les Terrasses de la Chaudière.
- $75,000 was allotted to HQ-SID for Information Technology (IT) security, for the purchase and implementation of Intrusion System Software, including the development of procedures and training of technical staff.
- $50,000 was provided for training mailroom and security staff in dealing with suspicious packages and emergency response measures.
- $50,000 in salary dollars were provided to shore up passport processing, personnel security screening and the NHQ Security lead role.

2002-03
In the fiscal year 2002-03 the security function submitted a business case seeking an additional $2,100,000 to support the resourcing of a national security organization for the department to respond to "September 11" type threats, to implement some requirements of the revised GSP and to respond to recommendations of the Year 2000 Security Audit. Ultimately, in the summer of 2002 the EMB approved $1,000,000 for the year to provide partial support of the initial security business case. It is unclear from the available documentation as to where specific responsibility for monitoring and reporting of benefits achievement associated with the business case proposal resides. Based on the accountability charter, it would appear that the implementation of the Departmental security program is the responsibility of the RDGs, with reporting on results being undertaken by the DSO for program monitoring purposes.

- $624,500 was approved for dedicated security officers in all regions and at NHQ.
  - $222,000 was allocated to 4 regions ($55,500 per region) for hiring a full-time security officer.
  - $78,500 was provided to another region for hiring a full-time security officer and a deployed site receptionist.
  - $324,000 was provided for NHQ Security to staff 4 security officer positions, including the Chief Security, Passport Officer, Ministerial Conferences Security Officer and BCP Officer.

- $140,000 was provided to EPS and ECS as supplemental allocations to assist in site security management.
  - $75,000 in Operations and Maintenance (O&M) was provided to EPS-Environment Technology Centre (ETC) for security guards and IT Security software.
  - $65,000 in salary and O&M was provided to the ECS-National Water Research Institute (NWRI) facility for clerical assistance in security management and an investment in an ID Card system.

- $119,000 was provided to CMC and HQ-SID for supplemental allocations to assist in IT security.

  - $81,000 in salary and O&M to the Canadian Meteorological Centre IT Security for upgrades to secure authentication system, for implementation of a DMZ system and for anti-spam software.
  - $38,000 in salary and O&M to HQ-SID to cover IT security duties.

Generally the stated deliverables associated with the funding were not addressed in the manner put forward. Of the regions, only Quebec Region actually hired a security officer at the stated classification level. Three other regions spent the allocations by understaffing or re-assigning resources, including the proposed lapsing of salary dollars, while one region had neither spent nor committed its allocation at third quarter (Q3). Both EPS and ECS appear to have spent or committed their allocations as predicted. NHQ Security converted the salary dollars for the BCP position into contract dollars for a BCP gap analysis study, as indicated above.

As of December 2002, many recipient areas had not had the approved funds transferred into their budgets. In addition, the tentative nature of the funding - i.e. current year, one-time allocation - resulted in uncertainty about future, on-going funding, particularly with regards to permanent staffing. NHQ manager has indicated that all regions were advised to fill the position; however, the final decision was left to the regions.

Other security-related funding - although not internally generated - included Effective Project Approval from TBS on a projected expenditure of $7,100,000 for work at the Canadian Meteorological Centre (CMC) in Montreal. This was required in order to relocate the existing Information Technology facility as a direct outcome of the risk assessment for the facility. The CMC supercomputer and telecommunications network is rated A1 in the context of civil or military conflict - the highest rating afforded to essential operations as determined by Department of National Defense (DND). As these operations require continuous service around the clock to ensure the delivery of essential services, the funding by TBS was essential to mitigate the risk.

2003-04

For the upcoming fiscal year 2003-04, the MAP Table has approved $1,000,000 on November 27, 2002, to signal support of the national security organization described in the business case. Environment Resource Committee (ERC) endorsement and approval in early 2003 would provide the Department with the human resources capacity to deliver physical security in each of the regions, at NHQ and in Environmental Protection Service-Environmental Training Centre (EPS-ETC) and Environmental Conservation Service – National Water Research Institute (ECS-NWRI) facilities. The funding would comprise salary and O&M allocations for a Designated Security Officer (DESO) position at an AS-04 level in each region, and Service owned facility (ETC, CMC, Canada Centre for Inland Waters & National Hydrology Research Institute (NHRI) to be appointed by the RDG or Senior Manager. It also includes four policy positions in NHQ.

Furthermore, the implementation of TRA recommendations was identified in the business case and would be pursued on a prioritized national basis subject to approval, otherwise individual facilities would be responsible for funding individual projects. Available

documentation did not clearly indicate how achievement of the benefits associated with the business case is to be monitored.

The Department's decision to fund the development of a national security organization is a critical step forward in addressing the strategic nature of security risk. It should be noted, however, that the present incremental funding approach and the existing accountability framework surrounding security management tend to compromise the effectiveness of current and future investments in security management.

Resourcing the security organization through a series of iterative funding proposals acts only to limit operational confidence in management's commitment to a permanent national security organization. This can be clearly seen in the hesitant and tentative manner in which the security community has responded to the provision of funds in 2002-03.

The accountability framework for security management at EC lacks the capability to influence and guide senior management on security matters, since there is little requirement for frequent and formal monitoring and reporting on the Department's security investment.

As noted earlier, the Business Line establishes and monitors departmental priorities and programs. These programs are implemented by Regional Directors General, who report directly to the Deputy Minister. Under the GSP, the DSO is required to establish and direct a departmental security program. The implementation of a departmental security program is to be accomplished through DESOs, who take functional direction from the DSO and line authority from the RDG. Without a clearly defined set of progress reporting guidelines and responsibilities, it is possible that the Department's investment in security management may not be adequately monitored. For example, funds allocated to the security community in 2002-03 for specific deliverables have not been consistently and specifically used for achieving those deliverables.

9.1 Audit follow-up recommendation 4

It is recommended that the DSO provide regular progress reports to MAP, and the EMB as required, on the status of on-going security program implementation.

9.2 Management Response

The DSO will provide quarterly reports to the Management, Resources and Results Committee, as well as annual reporting to the Deputy Minister.

Overall, the audit recognizes that the security community is addressing issues on a best efforts basis taking into consideration current HR resources available prior to the approval of the Security Business Case. It also acknowledges that post "9-11" communication and cooperation among EC's security community have increased, as well as renewed leadership from the National Security Office due to increased capacity at the headquarters level.

III. Conclusion

The audit follow-up recognizes that the EC security community has coalesced somewhat in the intervening time since the Security Audit of 2000. Cooperation and communication have improved -- a change generally credited to renewed leadership from NHQ security and a re-engagement to security risk management at the regional and Services level following "9-11". While acknowledging that the Department's matrix management approach makes management of a departmental program such as Security more challenging, the security function has vigorously pursued the need to establish viable resourcing scenarios in order to resolve fundamental issues of security organization and administration within the Department. It is apparent, then, that the security community has undertaken the challenge of its task on a best efforts basis and currently requires continued senior management's engagement to successfully achieve departmental and government objectives for security management.

The three recommendations from the Security Audit of 2000, where effective action is still pending, can only be resolved through senior management's continued attention and commitment. The Security Business Case process has started to address the operational risks, and now urgent attention needs to be directed to the strategic investment in the accountability framework for security management within the Department.

Appendix A
Accountabilities Charter

(Approved by EMB May 2002)

Authority is the power to make certain decisions and/or perform certain tasks within defined limits.

Responsibility is the duty to perform certain tasks.

Accountability is the obligation to answer for the performance of responsibilities. To be held accountable, an individual must be provided with the authority, the resources and responsibility for a task, output or result.

Authority, responsibility can be delegated but accountability cannot.

DEPUTY MINISTER

- Accountable to the Minister, to the Clerk of the Privy Council and to the Governor-in-Council, in accordance with existing Acts and rules.

EXECUTIVE COMMITTEE
PREVIOUSLY KNOWN AS EMB

Supports the Deputy Minister in the management of the department.

- Sets departmental strategic direction, policies, priorities and results and reconciles priorities and directions across Business Lines when required
- Supported by the ERC, makes decisions on departmental resource management strategies, multi-year departmental resource allocation and resource re-allocation between Business Lines/organizations
- Reviews the overall performance of the department and takes corrective action as required

BUSINESS LINES

TABLES, the management committees of Business Line (BL)**,** set directions, priorities, strategies, resource requirements, performance measures for the delivery of their respective key results and ensure horizontal management of issues; approve shift of resources within the Business Line to support the delivery of results.

Business Line Leads[2]	**Business Line Members**[3]
• Provide Business Line HORIZONTAL LEADERSHIP to bring focus on the delivery of results and build support and shared ownership among EMB colleagues of Business Line direction, strategies and priorities • Ensure that a BL Plan is developed, approved by BL members, its implementation monitored and corrective action taken as required • Ensure that specific results and commitments identified in the BL Plan are appropriately reflected in performance contracts • Provide guidance on the allocation of BL resources for the delivery of results	• Exercise HORIZONTAL LEADERSHIP and are accountable for the delivery of specific results and commitments identified in Business Line Plans • Actively participate in and influence BL planning, resource decision-making

[2] ADM EPS, ADM ECS, ADM MSC, ADM CS

[3] All ADMs, DG HR and RDGs

• Chair Table meetings to manage Business Line and create support mechanisms to BL as appropriate • Ensure complementarity between BLs • Bring the BL view point to EMB decision making • Bring solutions to DM when consensus can't be reached by the Table on resolving significant BL policy or resource issues	and negotiation of accountabilities • Bring organizational perspective to Business Line decision-making • Ensure linkages between BLs

ORGANIZATIONS

The organizations are the delivery mechanism of the business of the department. ADM and RDG provide VERTICAL LEADERSHIP within their respective organization and are accountable to the Deputy Minister.

Assistant Deputy Ministers	**Regional Directors General**
• Provide FUNCTIONAL LEADERSHIP[4] and guidance/support to organizations (Services and Regions) to ensure national coherence and consistency in achieving results and in the delivery of programs and services; develop policies, procedures and standards to support priorities, strategies and results set by BL and ensure their implementation • National lead on specific / assigned files[5] • Represent EC nationally and internationally and build partnership to advance results • Organizational management including the evaluation of their respective staff	• Manage the combined impacts of the 4 Business Lines priorities and resource decisions on the delivery of results in regions and ensure that regional integration of resources, results and regional priorities are consistent with BL priorities, strategies, results and commitments. • National lead on specific / assigned files[4] • Represent EC interests and policies regionally and on occasion, internationally and build partnership to achieve results • Bring regional perspective to influence national priorities/files • Organizational management including the evaluation of their respective staff

[4] Functional leadership is also exercised at the National Director General and Director level.

[5] Horizontal or functional leadership is exercised by national leads on a specific or an assigned file as determined by the Deputy Minister or EMB.