DEPARTMENT OF FOREIGN AFFAIRS AND INTERNATIONAL TRADE

AUDIT OF SECURITY

June 2000

Office of the Inspector General - SIV

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

Background

In July 1998, the Departmental Audit and Evaluation Committee (DAEC) tasked Internal Audit to conduct an audit of security. The assignment encompassed the security of information, personnel and property at Headquarters (HQ) and at Missions. A preliminary survey was conducted in the fall of 1998 and a report submitted to a Steering Committee established to review the results and recommend further audit work.

Audit Scope and Objectives

The scope of the audit addressed those activities, conducted at HQ and abroad, that lead to the implementation of security measures to safeguard information, people and property.

The objectives were:

1. To review the security risk management process;

2. To identify responsibility and accountability for the effective management of the process;

3. To determine what and where the costs of security are, how these expenditures are managed, and how the budget accountabilities link to the decision making process.

Preliminary Survey Findings

The Preliminary Survey raised *** major concerns:

***

***

***

Steering Committee Discussions And Conclusions

The Steering Committee discussed the Preliminary Survey and raised a number of additional concerns including:

- problems with the current security decision-making process;
- the need to determine where accountability for security decisions should lie;
- the need to determine where the current funding authorities exist and what changes should be made;

***

- the need to understand and make effective use of threat and risk assessments;

***

- the problems with security 'cost models'; and,
- what future security issues should be taken into account.

The Steering Committee concluded that further audit work was required to address these concerns and to support the preliminary survey findings.

DFAIT'S SECURITY ENVIRONMENT

The following elements summarize key financial data and management benchmarks used to define and analyse the environment in which DFAIT manages security responsibilities.

Costs of Security

The Departmental cost of security *** establishes a relative magnitude of security expenditures via-à-vis overall Departmental expenses.

Summary of Security Costs:

***

More details and analysis of these costs are found in Annex A of this report.

Treasury Board's Government Security Policy

The Government Security Policy (GSP) is a key security management reference. *** The GSP identifies the policy requirements for security risk management, and assigns responsibilities to DFAIT to protect sensitive information and assets under its control in Canada and at or between Canadian Diplomatic and Consular Missions.

The Government's Comptrollership Initiative

Recent years have seen a greater emphasis in government on Comptrollership initiatives. The key elements of Comptrollership are found in a recent document - The Report by the Panel on Modernization of Comptrollership in the Government of Canada - which stated that:

> "Modern comptrollership is about ensuring (amongst others) that: a mature risk management environment is created and sustained; and, that control systems are appropriate to management needs and risks".

The same could be said for security risk management. The key is:

> "..creating an environment in which taking risks and the consequences of doing so are handled within a mature framework of delegation,..."

ISD' s January 1999 Submission to Executive Committee

In January 1999, the Physical Security and Personal Safety Division (ISR) of ISD submitted a paper to Executive Committee on Security Management at Missions. This paper contained the following guiding principles:

- ***based on an improved Threat and Risk Assessment***

- "Senior managers and Heads of Mission should be held accountable for maintaining requisite security measures"; and,

- "ISD Bureau should enhance the process of consultation with Bureaux to identify and review the threats and risks that confront Missions, to ensure the most effective management of security protection decisions including those affecting resources."

The audit team supports these guiding principles and believes that the findings, conclusions and recommendations of the audit are compatible with them.

OVERALL AUDIT CONCLUSIONS

The overall conclusions of the audit are:

a) Effective management of security requires the pro-active involvement of Program Managers working with security, informatics and property specialists. While all these

groups need to provide input, one group must be identified as being accountable for the decisions taken.

b) The need for security measures is a result of, or driven by, operational decisions. ***

c) The concept of "user pays" enforces discipline on users of corporate assets by making them responsible to fund them. *** Missions pay some of the security costs related to their decisions, but others are paid by a variety of groups at headquarters.

d) ***

e) There are options to the current security resource management practices, but they are not simple and will require redefining the roles and responsibilities of functional and Mission Program Managers.

f) In situations where the "user pays" concept is not appropriate, a challenge function should ensure that the safeguards chosen to mitigate the security risks have been subjected to a cost-effectiveness analysis. ***

g) ***

RECOMMENDATIONS

The key recommendations of the audit focus on accountability and resource management and are addressed to the Departmental Executive Committee. These key recommendations as well as more detailed supporting recommendations are presented below.

Key Recommendation 1

***

Key Recommendation 2

Confirm that the Security and Intelligence Bureau (ISD) is responsible for developing corporate security policy in a changing global environment, * but that it does not retain any operating responsibilities or associated funds which would tend to violate the "user pay" process, except for funding inventories.**

Supporting Detailed Recommendations

2.1 Invoke the "user pays" concept of funding responsibility for expenditures***

2.2 Hold ISD accountable for:

- developing and enunciating security policy and standards for information, personnel and property;

***

- generating costed options for security safeguards; and,
- documenting buy-in and sign-off by geographic DGs and HOMs for the selected security options.

2.3 Assign ISD the responsibility to develop and conduct a revised approach to threat and risk assessments which:

- involves program managers at HQ and Missions for program assessments, support systems assessments, and site specific assessments; and,
- includes the development of cost-effective risk-management solutions.

2.4 Establish a forum of program interests (DFAIT and Other Government Department (OGD) program managers), chaired by ISD, to conduct regular discussions on changing security sensitivities, threats, vulnerabilities, risks and safeguard requirements, particularly those affecting programs delivered at Missions abroad.

2.5 Establish, implement and monitor service standards for ISD's corporate security support activities, from policy and standards development to Threat and Risk Assessment (TRA) provision, inspection visits and security equipment provision.

2.6 Develop a compendium of best practices in ISD for reference purposes when matching security vulnerabilities and threats with safeguard requirements.

2.7 Develop, confirm and implement management accountability frameworks for ongoing security related decision making processes such as:

- Enhanced Reliability Checks (ERC) for Locally Engaged Staff (LES)
- Mission security inspections
- Chancery leasing and construction
- *** design and development

2.8 Implement one of the following options:

a) Provide Missions with the funding for Military Security Guard (MSG) salary and allowance costs. Hold HOMs accountable for all security guard decisions, with ISD having the functional role of advising, monitoring and reporting to higher authority where differences of opinion arise. (Preferred option)

Or,

b) Assign ISD the full responsibility and accountability for determining and meeting all Mission security guard requirements (MSG, LES and contract), and allocate the associated funding, including housing, to ISD.

2.9 Provide ISD with a sufficient inventory base whereby they purchase and warehouse those items of critical security equipment which may be necessary to meet Mission and HQ security requirements on a short notice or 'just in time' (JIT) basis, but charge out to Missions the cost of any inventory items provided to them.

2.10 Where armoured vehicles are assigned, funding for the local operating costs should be reviewed to ensure that appropriate support for the continued readiness and usefulness of the vehicles is maintained. ISD is to provide the conditions under which these vehicles are purchased along with the minimum maintenance requirements. Geographic branches and Missions need to be funded for this “user pays” approach.

2.11 Establish purchasing and asset distribution policies, guidelines and practices which apply the ‘user pay’ concept, and will meet the intent of the upcoming accrual accounting policies and practices. At the same time, implement a charge-out process which allows ISD to maintain appropriate inventories of key property security equipment and provides for users to pay for such equipment when acquired from ISD.

2.12 Define the property security hardware and equipment, and the related funding, for which ISD will be held accountable.

2.13 Confirm the role of ISD as purchasers, warehousers and suppliers of specified property security hardware and equipment, but that user requirements are paid for by the unit/Mission involved. This option is intended to foster a joint cost-effectiveness risk-management option discussion between the users and the security specialists.

2.14 Consolidate the HQ management of personal safety radios to maximize service capability while minimizing costs.

Key Recommendation 3

***

Supporting Detailed Recommendations

***

Key Recommendation 4

Confirm that while the Physical Resources Bureau (SRD) is accountable for major chancery leasing and construction management, the Geographic and Program bureaux or OGDs as applicable, are responsible for the formal sign off of the SRD funding required to meet Program and Mission requirements. This is required to ensure that not only minimum facilities configurations based on ISD standards are implemented, but also; that any special program needs are duly authorized.

Supporting Detailed Recommendations

4.1 Assign accountability for decisions that influence the security requirements for ***personnel and property construction to those whose operational decisions drive the security requirements.

4.2 Assign funding responsibilities for Mission property security safeguards either with Missions, SRD or ISD. This must separate the funding responsibilities for corporate-wide security initiatives from ongoing security maintenance responsibilities, both at HQ and for Missions. The IDACS upgrade initiative is an example of a corporate security initiative that is funded centrally by ISD. However, adding IDACS to a new chancery is funded by SRD as an element of the total construction or leasing project.

4.3 Match accountability for property security safeguards with funding authorities, ensuring that the recipients of the hardware concur with the safeguard choices made.

4.4 Develop accounting policies for property security equipment and hardware that will meet the future requirements of accrual accounting and comptrollership.

Key Recommendation 5

Institute mandatory security awareness and training programs for all staff at HQ and Missions, with periodic competency testing required for specified positions.

Supporting Detailed Recommendations

5.1 Expand the coverage and content of existing ISDT security awareness and training programs for all staff at HQ and Missions. Require attendance for specified positions. Focus the training on security safeguard responsibilities and accountability when designing, developing, implementing and managing program operations, support systems, information and asset utilization.

5.2 Conduct competency testing, by ISD, of incumbents of designated positions ***

ANNEX A
DETAILED FINDINGS

POLICY AND REGULATORY FRAMEWORK

This part of the report provides details on the references for bench marking security risk management, our findings on accountability for security risk management decisions, and our general findings regarding security resource management decisions.

We have collected data on the costs of various categories of security-related activities within the Department, including those incurred abroad. The practices in place for deciding who should pay for expenditures is discussed, along with options where appropriate.

References For Security Policies And Risk Management

1. Treasury Board's Government Security Policy

The Government Security Policy (GSP), as a key security management reference, provides considerable direction for developing recommendations related to this audit.

The GSP's primary objective is: *** Further, the GSP describes Security Risk Management in terms of the following key tasks:

- Analyse and assess threats and risks to which sensitive information and assets are exposed,
- Select risk-avoidance options,
- Implement cost-effective safeguards

The use of references such as "appropriate safeguarding", "select risk-avoidance options", and "implement cost-effective safeguards" all indicate that security risk management is not black and white but requires the balancing of risks with costs.

The GSP also assigns seven key responsibilities to DFAIT, four of which are directly related to this project.

a) All measures to protect sensitive information or assets under its control in Canada, and at and between Canadian diplomatic and consular Missions abroad.
b) Conducting or arranging the inspection of the above measures.
c) Providing advice on threats to sensitive information and assets outside of Canada, when requested.

d) Providing protection to Canada-based staff and their dependents at Missions abroad and to locally engaged staff while working within the Mission.

The above GSP references provide adequate guidance for the audit to assess the current situation and to develop an improved managerial framework for security risk management in DFAIT. Accordingly, the audit will address security requirements and responsibilities of OGDs conducting Program operations at Missions abroad, as well as our own security responsibilities.

2. The Government's Comptrollership Initiative

In recent years the government has placed greater emphasis on Comptrollership initiatives. The key elements of Comptrollership are found in documents issued by Treasury Board. Two of these elements are risk management and control systems. In addition, in 1994, the report of the Office of the Auditor General (OAG) on DFAIT spoke about the need to manage risks and to understand the financial implications of decisions before they are taken.

As with many recent management initiatives, the need to match accountability for decisions with program and financial authority has been continuously emphasized. However, the climate which allows this to take place must be present. The Report by the Panel on Modernization of Comptrollership in the Government of Canada stated that "Modern comptrollership is about ensuring (amongst others) that: "a mature risk management environment is created and sustained"; and, that "control systems are appropriate to management needs and risks". This, of course, includes security risk management.

Those who benefit from, or require the need of, security safeguards should have input to determining the appropriateness of the safeguards proposed. They should also be accountable for balancing the level of risks with the cost of the safeguards required, and for defending the accepted option.

There are two types of risk involved. The first is preventative risk management, and involves balancing the initial risks of exposing our information, people and property with the cost of safeguarding such assets. The second is corrective action risks. This involves balancing the effort and costs of implementing preventative safeguards against managing the efforts and costs of taking corrective action should our assets become compromised.

The key is "..creating an environment in which taking risks and the consequences of doing so are handled within a mature framework of delegation..." A mature framework for security risk management decision making is needed to foster the necessary changes in DFAIT.

3. ISD' s January 1999 Submission to Executive Committee

In January 1999, the Physical Security and Personal Safety Division (ISR) of ISD submitted a paper to Executive Committee on Security Management at Missions. This paper contained the following guiding principles:

- *** based on an improved Threat and Risk Assessment model;"

- "Senior managers and Heads of Mission should be held accountable for maintaining requisite security measures; and"

- "ISD Bureau should enhance the process of consultation with Bureaux to identify and review the threats and risks that confront Missions, so as to ensure the most cost-effective management of security protection decisions."

4. A Proposed Risk Management Accountability Framework

Normal audit practice requires the development of subject matter audit criteria, benchmarking and/or references against which the audit subject is assessed. However, management of security in an international governmental environment limits the use of traditional audit practices for this particular audit. *** DFAIT must define its own security management framework given its own management philosophy and program interests.

Regardless of the variables in program interests, establishing a framework from which security management decisions and accountability can be formulated involves the following key processes:

- Determining program integrity sensitivities, threats, vulnerabilities and risks.
- Obtaining and analysing collective program and site specific security-related information.
- Determining program integrity safeguard options.
- Determining and costing the various options to mitigate security risks.
- Selecting and approving cost-effective safeguards.
- Assigning funding responsibility to match security accountability.
- Implementing security safeguards.
- Reviewing effectiveness of action taken and adjusting, as necessary.

The above framework has been used to guide the review and assessment of the present management of security in DFAIT. However, the framework itself has yet to be proposed and accepted as the basis for security management within the Department.

ACCOUNTABILITY

Accountability for Security Risk Management

The review of the management processes involved in security risk management found a variety of cases and processes where accountability was misplaced or abdicated (see Appendices B and C).

In various situations, accountability for security decision making was assumed by, or considered to be the responsibility of, those having the mandate to provide security policy or to monitor the presence of a secure environment at Missions. Accountability was not generally identified with those who require the safeguard to protect their programs, information, people and assets.

Accountability for security policy development, for the interpretation of security policies, and for monitoring the implementation of, or maintenance of, safeguards is generally accepted as belonging to ISD, through ISC and ISR. The credibility associated with conducting such functions, however, is in dispute.

Accountability is not clear, though, for the following security risk management tasks:

- Who selects (presents/determines) the risk avoidance options which could be implemented?
- Who decides and commits the organization to the most cost effective solution?
- Who accepts the appropriateness of the safeguard?
- Who accepts accountability for the presentation and defence of the optional safeguards chosen (for resource decisions) to senior management?

The cases studied and processes reviewed during this audit indicate a strong absence of accountability for security risk-management decision making in the hands of those who manage programs abroad.

Assessing Security Threats, Vulnerabilities and Risks

Interviews, anecdotes and the initial DAEC mandate, offer perceptions that the security solutions applied exceed what is necessary and are costly and burdensome.

To demonstrate that security services facilitate the achievement of program objectives, and avoid the imposition of unnecessary/burdensome controls, suggests there must be discussion between program managers and security specialists. These discussions should focus on the sensitivities, vulnerabilities and risks associated with programs, information, personnel and property. For example: what is their nature? Are they event

driven (temporary) or ongoing? Assessments and discussions on available options to mitigate such risks should follow. Finally, appropriate safeguards must be selected .

Those who have been affected by the solutions implemented have expressed dissatisfaction with the appropriateness of these solutions, which are perceived to have been imposed. Mission program managers and some functional program managers who currently are charged with funding the solutions have expressed these frustrations.

The issue of how solutions were developed has been questioned. A key concern is who has the authority to decide on the safeguards needed to mitigate specified threats, vulnerabilities and risks.

The lack of options to what has been proposed is another point of contention. The credibility, not the value, of the security function is at issue. Thus, accountability for determining the necessary safeguards has been deemed to be in the hands of the security specialists, or the functional specialists charged with implementing the solution. It is not considered to be in the hands of those accountable for the delivery of the programs at Missions and HQ - the very people who require the safeguards.

Missing from this equation is the acceptance of accountability for decisions arising from discussions between stakeholders. If the security specialists work with the affected program managers, to identify what security concerns exist and what optional safeguards are available, then the choice of the safeguard could be made by those affected by the decision, not those who identify the options or who currently fund the solutions.

Accountability for Funding Security Safeguards

Current Departmental practices reinforce the perception of imposed solutions by security specialists, further supported by funding mechanisms for supplying the solutions.

Presently, the funding of many security solutions in the Department is managed by those who identify the proposed solutions. This removes the very managers responsible for program delivery from the responsibility to defend the choice of safeguard. Examples exist of corporate IT and property specialists implementing and funding security safeguards for the protection of information, personnel and property. However, they are also expected to defend the costs involved. This becomes problematic as they have had little, if anything, to do with identifying the risks against which protection is sought. The program managers requiring the security safeguards have not had to account for and defend the funding involved. If they haven't had to pay for the safeguard, they haven't had to defend the decision, even if they benefited directly from it.

Numerous situations exist where the managers accountable for program delivery are not held accountable for resourcing the associated safeguards, nor is there any independent challenge of safeguards chosen and costs incurred. Appendix B provides examples of this phenomena. Managers ,therefore tend to suspect that safeguards are imposed and are not necessarily cost-effective for the risks and vulnerabilities confronted by the programs being conducted within their organization.

In practical terms, when the security specialist defines security policy, identifies risks, then selects and pays for the safeguards, why is management intervention required? Challenge functions at the planning stage exist in other Departmental resource management functions, with the accountable managers having to defend their decisions. For security specialist decisions there may very well be internal challenge mechanisms within ISD. However, these processes are not evident to the clients who are affected by the decisions.

The Contract Review Board, the Canada Based Staff placement process, approving audit and evaluation program funding by the DAEC, the Long Term Capital Plan and the Information Management Plan are all examples of funding proposals that face challenges by independent sources. Ultimately, the manager involved has to make, and take accountability for, the resulting decisions. The purpose of the challenge function is but to ensure that all options have been given due consideration.

By not placing financial accountability for security safeguard decisions on the shoulders of the manager responsible for program delivery, the potential for the cost-effective implementation of safeguards is reduced. Providing an independent source of review for security safeguard funding decisions could bring objectivity to a risk-sensitive function.

MANAGEMENT OF SECURITY COSTS

Introduction

The Departmental cost of security is estimated to be at least*** Security includes all activities intended to protect our information, personnel and property. While this ***figure does not include some costs which the audit team was unable to estimate, its presentation is beneficial for two reasons:

- it establishes a relative magnitude of security expenditures vis-à-vis overall Departmental expenditures; and

- the exercise indicates the extensive and pervasive nature of security and the variety of Departmental groups that fund security requirements.

The specific items included in this figure are identified in the cost summary below. To select which costs to include, the audit team began with the premise that if the Department had no concerns for security, its costs would be much lower. The task was then to identify the costs that were attributable to security activities, because the Department does not function in a world without such concerns.

The audit team initially assumed that operating and capital expenditures in 1997/98 were probably representative of on-going operations and were used where available. Where 1998/99 values were found to be more representative, those figures were utilized. The precision of some of the other figures cannot be guaranteed as many are 'imputed', such as average costs of housing at a particular Mission, and average compensation costs for specific employee groups. In addition, the financial coding for some expenditures did not distinguish secure from non-secure categories, and therefore these costs are not included. The intent is to provide an estimate of security-related costs to understand the relative magnitude involved.

It should also be noted that DFAIT is responsible for security for all Programs at Missions, including OGD's. No consideration is made for any past agreements with other departments that may have transferred funding for some security costs into DFAIT's base reference level. The figure does not include the cost of*** There is no allocation of the costs of Departmental or OGD staff who spend only a portion of their time on security support services. Other corporate overhead costs that might be attributed, such as finance and personnel, are also not included.

Our analysis of security costs demonstrates a considerable dispersion of the types of costs involved, where the costs are incurred, for what security purposes, and who has authority to spend the funds. Our interest was only with the salaries and benefits, operating and capital costs that were dedicated solely to security. Included are: security guards of various types at HQ and Missions;*** corporate security direction for policy,

standards and monitoring;*** and support;*** Specific property capital and maintenance costs associated with security safeguards could not be easily identified, and therefor a value for these costs is excluded from the cost summary. ***

SECURITY COST SUMMARY

The following is a summary of the costs of security, by category:

***

Refer **Table 1,** below, for more details on the cost categories and the funding sources.

COST ANALYSIS

The following sections provide a more detailed analysis of the various cost categories. Also provided are the current expenditure accountability structures associated with these costs and the impact of the present funding arrangements.

Due to the homogeneous nature of the expenditures, each category is addressed independently from the others. However, the principles of security risk management and comptrollership, described earlier in this report, are applied to all categories regardless of the nature of the current funding arrangements.

Table 1 - Costs of Security Activities
(Millions)

	Totals	HQ		MISSIONS			Line Totals
		Staff Costs	Other	Staff Costs	Housing	Other	
SECURITY GUARDS Contracted Security Services MSGs LES Security Guards, Uniforms	***	***		***	***		***
SECURE COMMUNICATIONS Missions (***) Housing,etc. SXD (SXTC, SXTT) Operating and Capital	***	***	***	***	***		***
CORPORATE SECURITY DIVISION ISD - Staff Operating and Capital	***	***	***				***
SECURITY EQUIPMENT PURCHASES HQ acquisitions Crypto Repairs to security installations		***				***	***
DIPLOMATIC COURIER SERVICES	***	***	***				***
PROPERTY SERVICES Capital projects Property maintenance	***						
GROUP TOTALS		***	***	***	***	***	***
GRAND TOTAL	***						

SECURITY GUARDS

	Millions
HQ (includes Vanier, but excludes, CFSI, Protocol)	***
MSG salaries and allowances paid by ISR	***
MSG housing and support by Missions	***
Mission contracted security services	***
Mission LES security guards, uniforms	***
TOTAL	***

Missions are accountable for the LES and contracted security services *** Their budgets provide for these costs and they make the associated operational and financial decisions, with advice from ISD. ***

Issues

In the NCR, ISD incurs *** for Commissionaire security costs, but this does not include Commissionaires for CFSI, Protocol, and the Library. A previous study noted that a few years ago, Commissionaire costs of about *** were transferred from ISD to other budgets as part of an ISD security cost reduction exercise. In this scenario, costs were not reduced, but transferred to identifiable users.

This concept of "user pays" is applied at HQ but not entirely at Missions*** In a recent paper, ISD requested that Missions justify the presence and number of MSGs. This implies that Missions should determine whether or not MSGs are required. The audit team expects that ISD would provide expert security advice to the Missions during such an exercise, but, that ultimately, Missions would be held accountable for making the decision.

Impact

If Missions are to be held accountable for MSG security guard decisions, the total costs would be more easily identifiable if Missions were to fund the labour costs as well as the housing. The Missions could then have full budgetary control for local security services of all types - MSGs, LES and contracts. ISD would retain the security policy advisor and monitoring roles but leave the security risk-management decision making to each Mission.

Optionally, if ISD is deemed accountable for Mission security guard requirements, then ISD should be provided with the full funding to support, and defend, the risk-management decisions. The budgets for MSGs and their housing, the LES, and contracted security services would all be the responsibility of ISD.

In short, either the program manager (HOM) or the functional manager (ISD) is held accountable. There should not be a split responsibility for associated costs as this

approach leaves no one fully accountable, and thus reduces the likelihood of making cost-effective decisions.

In support of the “user pays” concept, the audit team refers to the current ISD unwritten policy which requires that Missions pay for any additional MSGs beyond the current ISD budgetary level. ISD charges the incremental costs to the Missions’ budget. This administrative process is no different than the current method applied for HQ Corps of Commissionaires costs for users other than LBP and Vanier HQ security, as ISD pays the Corps invoices but charges CFSI, Protocol, etc. for their Commissionaire costs.

Where HOMs are deemed to be accountable, through their Ministerial terms of reference, for the ..."staff's welfare, including the personal protection of Canada-based staff and their families" at the Mission, charging Missions for incremental salary costs of MSGs is an acceptable approach. This is in addition to housing costs already paid by Missions. No explanation could be found to support the separation of some of the MSG costs between ISR and Missions.

Should ISR have concerns regarding security guard decisions by Missions, their recourse would be to the Departmental Security Officer - their superior. This concept is similar to other functional support authorities within the Department, where the resolution of concerns is raised within the functional hierarchy.

SECURE COMMUNICATIONS

***

Table 2 - Secure Communications

Funding Source	Expenditure Category	Staff Costs ($Millions)	Other Costs ($Millions)
Missions	***	***	
	Housing, etc.		***
SXD	(SXTC, SXTT)	***	
	Operating and Capital		***
		***	***

The first major category is the Canada Based Staff at Missions who manage and maintain DFAIT’s secure systems overseas. This costs about *** for staff costs and *** for housing support for *** Systems Administrators and *** at *** separate Missions. One-third of the

staff is located at six sites. The Missions pay the full costs of these services, along with local support costs. There are other related expenditures such as equipment acquisition and repairs that are scattered amongst various HQ functional support units such as ISD, SXD and SRD. Missions also fund similar items, but the audit team was unable to fully segregate them in the financial accounts. The information gathered is discussed later in the section on Security Equipment Purchases.

The second major category is funded by the Information Management and Technology Bureau (SXD), via the ***. This provides secure systems design, development, implementation and life-cycle maintenance which costs about *** for staff costs and *** for operating and capital costs.

The equipment costs for *** are located in various organizations, depending on whether they were allotted units as part of a corporate initiative, were charged for incremental units beyond their allotment, or requested units on a site-by-site basis. The audit team was unable to determine with certainty that all such costs have been captured in the data in this report.

Issues

The cost of Mission *** services are linked to those where they reside. Some provide a regional service as well, while others provide support through hub and spoke arrangements. These technical security specialists are also supported by *** from HQ for specific project or inspection purposes, the costs of which are borne by the HQ home unit, either ISD or SXD.

Accepting the assumption that these people provide secure communications support for Mission programs, and given that these programs operate out of designated Missions, the principle of "user pays" still holds for these services. Again, the program requirements and the accountability for their funding are linked, with the Mission program presence being the rationale in general for the majority of such staff. As noted, some personnel are located for regional support purposes but it is not administratively logical to split their costs among the various Missions served.

***

Impacts

*** The source of funding would appear to depend on who has the available budget at a given time. Some Mission expenditures may in turn have been funded out of Area Management Advisor (AMA) offices, but we did not follow this up. ***

As the Department moves to accrual accounting, ownership of such capital equipment may force some re-thinking as to who should fund such expenditures. The need to identify and

budget for life-cycle management costs may influence funding policy decisions to a greater extent when accrual accounting *** must be considered.

When ISD is requested to supply or replace ***, the re-supply costs may be borne by ISD or the requesting unit. To our knowledge there is no hard and fast rule which defines whether the payment is made out of the ISD budget or that of Missions or HQ units. Generally if ISD recommends something during a security inspection, they pay for it.

Under this scenario the most cost-effective solution to these secure support services problems may not necessarily result. If Missions do not have to fund the acquisition, then they will likely accept what is provided as long as it meets their minimal needs. They need not give due consideration to the most cost-effective solution, as someone else is paying. This type of scenario is consistent with other categories of security costs as well.

CORPORATE SECURITY DIRECTION

The estimated cost for the provision of corporate security direction by ISD is *** - half for staff costs and the remainder for operating and capital budgets. *** The costs also do not include the *** MSG budget nor the *** Corps of Commissionaire budget. The Corporate security functions include, but are not limited to, the following:

***

- conducting physical security and personal safety inspection, monitoring and support services;

***

- providing various management and financial support services,***

The major cost components, other than unit staff salaries, are the operating and capital expenditures. Included are travel costs for Mission security visits, office administration, security training and awareness programs, and some costs of the acquisition, warehousing, shipping and installation of various security equipment for HQ and Missions.

Also included is the capital replacement fund for armoured vehicles of *** per year and the special budget for the IDACS installation and upgrade program of ***. (The total three-year IDACS project estimate was ***).

Issues

The audit team focussed on the acquisition, warehousing, shipping and installation of various security equipment for Missions. These activities stem from ongoing inspections, security needs identification and safeguard installations recommended by ISR functional

specialists. The concern relates to accountability for security safeguard decisions and the funding thereof.

When Missions are advised by the ISR *** that there are shortcomings in security measures, particularly those related to physical and personal security, the solution is usually specified by ***. In many such cases the equipment is supplied, installed and/or replaced from ISD's stock, or the project is funded out of the ISR budget. When Missions are advised that they need certain safeguards and ISR will provide them, Missions can distance themselves from responsibility for the costs. They don't have to pay for it, and if the application is seen as burdensome, it can safely be ignored once the 'monitor' has returned to Headquarters. The buy-in is not assured.

This approach does not meet the "user pays" concept mentioned in earlier sections. Neither is it consistent with the Mission's responsibilities to pay for security guard services and armoured vehicle support costs. The application of the "user pays" concept is selective, not consistent.

The rationale offered by ISD for the current approach is that by providing the funding for such safeguards it opens the door to acceptance of ISD's role in security management. The audit team believes that this approach does not enhance the credibility of the security function, which should be the key concern. However, when ISD recommendations are viewed by Missions as an impediment to their operations, they will challenge it. There is no challenge of the decision, nor the costs involved, when the Mission does not have to fund it themselves and/or the safeguard does not impede their day-to-day operations.

One recent example brought to the attention of the audit team was the case of a Mission's secure area door hinges which required replacement. The Mission was advised not to fix it but to wait for *** to visit the site, assess the situation and pay for the repairs. If the situation is obvious, should the Mission have to wait for an ISR visit before correcting the problem? Also, if the Mission requires the doors to operate properly should not the Mission pay for it? The logic of waiting for a visit so that ISR pays for it is questionable.

Impacts

In summary, with ISR defining and providing some security safeguards, the Missions are virtually removed from the decision-making process. They can consider themselves unaccountable for the risk-assessment and safeguard-decision process. And yet, they are the ones who will experience the benefits, or impediments, of these safeguards.

The audit team was advised of several cases where Missions have become concerned only when the safeguard recommended poses an impediment to the daily operations of the Mission. These scenarios are evidence of cracks in the security risk-management

decision-making process. The need to provide cost-effective security safeguard options has not been adequately addressed under these scenarios.

SECURITY EQUIPMENT PURCHASES

A variety of property, ***, parts and repairs totalling *** were acquired in 1997/98. Expenditures were charged to the following budgets:

ISR	***
SRD	***
SXD	***
Missions	***
Total	***

While eighty percent of the total expenditures were from HQ unit budgets, the majority of these expenditures were to fund Mission property security requirements. For some Mission projects, funds were obtained from up to four sources - their own, ISR, SRD, or SXD. The audit team was unable to gather information on the extent to which the AMA office contributed to these expenditures.

A cursory review of the types of costs found under different expenditure sources demonstrated IDACS costs in SRD and ISR; security equipment, windows, *** for Missions in SRD and ISD; security inventory acquisitions in ISR, such as ***; alarm systems in Missions;*** Not included in the above are minor parts and repairs that are paid for by the Missions associated with supporting armoured vehicles. The audit team had difficulty separating the costs included in this category of expenditures and those found in the Corporate Security Direction category. While some cost duplication may exist, it would not significantly affect the overall estimated figures, nor the prime concern for funding responsibilities related to security safeguards at Missions.

Issues

The main issue with respect to accountability is the apparent absence of any policies or guidelines that specify who is responsible to fund security safeguards at Missions. Without further analysis, it is difficult to determine who decided what security features were required and who really paid for them.

Another issue is inventory management. First, the information in the inventory system used to control the stock of security equipment maintained by ISD is only roughly accurate. Second, all radio units and parts are found in the SXD inventory, both new and used units. Funding for new or upgraded units is the responsibility of ISD, whereas repairs and replacements is the responsibility of SXD. Third, for radio systems recommended by ISD,

it is SXD which is responsible for assessing installation requirements and providing the units from its inventory. Should the funding from ISD not be available to re-stock new or upgraded radio units required by SXD, the audit tam was unable to determine how the inventory levels are replenished.

Impact

As security expenditures for similar equipment can be paid for by two or more organizations, accountability for incurring each level of expense cannot be tied down. ISD buys and warehouses equipment which is then shipped to Missions, who may or may not be charged for the items or the shipping. ISD may issue, from inventory, security equipment for new chanceries and ISD may charge directly for the equipment or credit the value to its inventory budget. The decision is made on a case-by-case assessment, which in the audit team's opinion does not comply with the principles of cost-effective budget management.

With accrual accounting to be implemented in the near future, the impact on HQ functional units and Missions, when authorizing security equipment, requires closer examination to determine how this new accounting requirement will affect each organization.

In summary, payment for these security expenditures is dependant on funding availability. Accountability for the decision becomes obscure because of the current process.

DIPLOMATIC COURIER SERVICES

The current diplomatic courier service costs the Distribution Services Division (SBG) a net *** per year, consisting of six couriers and a supervisor for a staff cost of about ***, with other operational costs, primarily travel, accounting for ***. The *** also includes the cost of shipping items via non-secure means, at approximately one third the cost of the "red bag" service. The total cost to the Department of the courier service is considerably higher than ***, as SBG recovers costs which are directly attributable to other users for significant demand shipments.

Issues

This service has experienced a major reduction over the last few years with a limited number of Missions now comprising the "core" service users. As mentioned above, other users avail themselves of the service on a cost-recovery basis as it provides the level of protection deemed necessary to deliver their "products". Consequently, the "user pays" concept applies in some cases to this security service.

The audit team assumed that any further changes to courier services would be based on decisions affecting the need for the delivery of designated secure materiel. The audit team did not review the operations from this perspective.

SECURE PROPERTY SERVICES

Property services of interest for this study apply primarily to the construction or lease of new chanceries or major renovations of existing sites. Also of interest are the maintenance and repair functions performed by the ***, specifically as they relate to security expenditures.

Chanceries

The nature of security requirements for chanceries is based on a variety of factors stemming from the security threat and risk assessment (TRA) for the given location. Depending on individual program requirements,***, the combination of these programs coupled with the country and site location of the chancery all have an impact on the construction security requirements.

Program demands for communication and physical access and restrictions (control extremes) combine to present scenarios which define minimal to optimal security requirements. The greater the need to restrict or control access, due to risk sensitivities, the higher the cost.

Security risk management for chanceries involves:

- the appropriate definition of program requirements;
- the analysis and assessment of sensitivities, vulnerabilities and exposure risks;
- the selection of risk-avoidance options (key), and;
- the implementation of cost-effective solutions.

These risk management criteria are consistent with the requirements of the Government Security Policy and the Comptrollership initiative.

Issues

DFAIT, as the employer, must within reason, provide Mission staff, and CBS families with the same measure of personal safety that government employees would enjoy in Canada. Program needs have little to do with the primacy of ensuring personal safety for Canadians assigned to represent their country abroad.

According to SRD, there is really no single basis for estimating the annual costs of property service security. Circumstances vary from site to site. For instance, the cost of a blast resistant (BR) wall in Jakarta is different than the cost of a BR wall in Bogota. In addition, the security need varies considerably from site to site. SRD does not determine that need.

There are certain inescapable costs associated with operations abroad. SRD developed a presentation that demonstrates the additional cost of delivering a construction project abroad compared with delivering the same facility here in Canada. However, the total costs to the Government of operating abroad vary according to a number of factors; the real estate market prices and availability of suitable facilities are two such examples.

***

***

SRD has considerable difficulty in isolating security costs within its overall program costs. The Bureau, for example, spends considerable money on projects that are not construction projects. Security is also a major factor in leasing projects. And when SRD is looking at options and narrowing down alternatives for accommodating Mission programs, security considerations are also factored into their decision making.

The chancery project management process currently in place involves the participation of various functional specialists in security, *** and property, as well as geographic and OGD program interests. The audit team has not questioned this project management process due to the highly positive feedback from the various parties involved. The one concern

raised by stakeholders is that accountability for the costs associated with the projects are expected to be defended by the functional specialists. ***

Impacts

Accountability for security decisions should be traceable to those who define the requirements. This aspect is not easily identified within the DFAIT decision-making framework as it relates to chancery acquisition, leasing or construction. However, unless it can be determined who is responsible for deciding the requirements, who is held accountable for the decisions, and who must defend the funding thereof, then implementing the most cost-effective solutions and obtaining evidence of the effort taken to do so may be difficult to achieve.

PROPERTY MAINTENANCE AND REPAIRS

*** SRD conduct periodic visits to their geographic areas of responsibility. Their scope of responsibility, amongst other duties, is to assess the state of property maintenance and the structural health of chanceries, official residences and staff quarters. Recommendations for improvements are prepared based upon site visits, and in some cases, requests from Missions to upgrade, replace or repair property holdings. Funding becomes the critical issue at this point.

Issues

The audit team's analysis of the 1997/98 expenditure data has found that property security safeguards are also included in the list of property improvements which have been addressed by SRD at the Missions. In earlier sections of this report, it is noted that SRD financed a variety of security measures at various Missions, including IDACS, security windows, etc. These same types of expenditures were also incurred by ISD at various other Missions.

The audit team is not aware if any policy or practice exists whereby the funding accountability for Mission property security expenditures resides with one DFAIT unit. If various units provide funding for similar security requirements, it is difficult to link accountability for the results to the implementation of the most cost-effective solutions. In recent case studies, security specialists made recommendations affecting security equipment and either: a) paid for the secure equipment, shipping and installation; b) authorized the work and requested others to provide the funding, or, c) separated the high cost from low cost items and split the funding requirements. The audit team found no evidence of a consistent approach.

Impacts

The evidence indicates that the most cost-effective solution is not necessarily discussed and agreed to by the recipients. In addition, it appears that funding decisions depend more on the availability of the money than on the need to identify cost-effective solutions. Based on the evidence that there are too many instances where funding availability has driven the end result, the audit team cannot state with any degree of certainty that cost-effectiveness is the prime criterion for security safeguard decisions.

Background working Papers

In Annex B, we outline specific cases chosen for study as examples of the various decision making practices related to security risk management experienced within the Department, both at Missions and HQ. We also provide in Annex C an overview of the LES Enhanced Reliability Check (ERC) process that is encountered on an ongoing basis. Some of these circumstances may call for further initiatives to foster understanding of the roles and responsibilities of all parties and lead to more informed decision making when security of information, personnel and property are involved.

ANNEX B
CASE STUDIES

This annex provides examples of recent cases involving security issues where accountability for the decisions taken has not been clear, or where there were practices which were not in the best interests of the Department from a security risk management perspective.

CASE STUDIES PRESENTED

***

***

This annex reviews the process involved when hiring LES staff at Missions, as Enhanced Reliability Checks as required. This process is presented to raise awareness of the responsibilities of Program Managers at Missions when involved in hiring or re-assignments of LES staff.

LES SECURITY CLEARANCE (Standard Enhance Reliability Check Process)

Background

The Government Security Policy requires that DFAIT conduct an Enhanced Reliability Check (ERC) on any individual whose duties or tasks involve access to designated information or assets. In 1998 there were about 1,500 ERCs processed, which does not include updates required every 10 years.

The use of LES at Missions has increased over the years due, in part, to a reduction in CBS postings. ***

Process

***

ISR/992-7996***

SIX

MHS

UNCLASSIFIED

1-11-ISR

RESPONSE TO THE SECURITY AUDIT OF 1999

Januay 19, 2000

MHS-0015

2

In the attachment to this memo, I am providing a response prepared by the Security and Intelligence Bureau (ISD) to the July 1999 report of audit of security that was undertaken by SIV.

MKM
MSL
ISD
SRD
SRS
SXD
SXT
SIV
SMD
TBD
JPD
ISR
ISDF
ISDT
ISC

1. The report of the audit confirmed a number of current practices in the management of security in the Department of Foreign Affairs and International Trade, and made a number of recommendations designed to tighten accountability for security in the department.

2. While many of these recommendations have been timely and useful, and have already affected the daily operations of the Security and Intelligence Bureau, we disagree with a part of a key recommendation (Key Recommendation 2), namely that the ISD Bureau "not retain any operating responsibilities or associated funds which would tend to violate the "user pay" process, except for funding inventories. Our disagreement with this part of the recommendation came after a round of consultations with the "users" - principally the Physical Resources Bureau (SRD) and the geographic Area Managers. It was agreed that a wholesale move in this direction would undermine entirely the department's ability to maintain requisite standards of security and would simply introduce new disconnects in accountability for and management of security.

3. In the spirit of this recommendation, however, we have actively sought to identify better ways of consulting on security issues with "users" and better documenting the process of decision making on security. Much of this process is described in our response and the follow-up action plan.

4. Also attached to this response is a table designed to show with greater clarity where the principal centres of decision-making on the great variety of security procedures, systems, equipment and standards are located. As with all undertakings in this department, the process is complex, reflecting a complex department with complex needs. With this table, we hope to ensure that the complexity of identifying and responding to security needs does not contradict the requirement for careful accountability and sound decision-making.

Hugh L. Stephens
Assistant Deputy Minister
Communications, Culture
and Policy Planning

Response to the Security Audit of July 1999

The following is the response of the Security and Intelligence Bureau (ISD) to the Security Audit of July 1999. All recommendations put forward by the audit team are addressed, although not all solutions proposed by the team were found to be practical. One or two have significant resource implications which may delay implementation.

The audit was limited to a review of the management of responsibility, accountability and decisions on expenditures related to security in the Department. It made no observations on the effectiveness of the security program in identifying risks to security and personal safety, selecting options for risks and protective measures, and the administration of these measures.

Consequently, in responding to the various recommendations as the bureau responsible for the delivery of the security program, we have taken the liberty of injecting some judgments on the effectiveness of current practices. In this respect, we disagree with a small number of the recommendations.

The audit steering committee (as mentioned in the audit report) identified a number of related issues that would benefit from further audit work. In the full knowledge both that security is an imprecise discipline and that security threats are constantly changing in nature and location, we welcome ongoing investigations into the manner in which security is planned, budgeted and managed in the Department of Foreign Affairs and International Trade. We look forward to cooperating in any further study that the Inspector General may wish to undertake.

Overall Conclusions

The audit comes to a number of conclusions regarding the importance of applying the "user pay" principle to all operational aspects of security, with the exception of some centralized systems - such as communications - where the integrity of the corporate system must override both responsibility and control in the hands of the "user".

This does raise the question of who the "user" is in a worldwide corporation such as DFAIT staffed largely by rotational personnel. If one speaks of the security of missions, is the "user" only the incumbents of the day, in which case standards of security could gyrate widely? Or is the "user" the department as a whole responding to global standards of security (likely not the intent of the audit)? Or is the "user" the team of managers and decision-makers that include geographic bureaux, area managers, HOMs and program managers?

We believe that the primary "user" of security is the last of the three definitions. In support of these "users" the Security Divisions reporting to the Departmental Security Officer (ISD) provide

specialized resources in the way of definition of standards, technical expertise and the management of corporate security systems as identified in the audit and in our Annex I (see below).

We have been assured that the intent of the audit is to ensure that there is *accountability* for the resource decisions that are made in the department in the name of security. In order to impose a clear *process of accountability* for management of the various security functions in the department, it is important to identify the range of these functions and where responsibility lies.

The requirement for a clearer definition of responsibility and for a better accountability process have led us to design a matrix of responsibilities. In our *Annex I,* we have attempted to break down responsibilities in somewhat greater detail, and have identified where responsibility (and spending authority) should be located.

In some cases, this division of responsibility represents current practice in the department. If we applied the recommendation to shift responsibility for "security installations and equipment at missions" to users, this would imply a major change. Some years ago, the Security Division (now ISR) was granted a reference level capital budget designed to assist missions around the world bring security installations (such as access control barriers) and equipment (shredders, alarm systems, locking devices) up to standard in the face of advancing globalized threats to the security of our missions and the safety of our personnel. After thorough consultation with geographic Area Manager Advisors, we have agreed with their advice that such a capability should remain with the security bureau, but that regular and structured consultations with the geographics should take place to ensure that security needs are met in a timely fashion and that the "users" agree with and understand the need and function of any new security installations.

As there are so many points of overlap when it comes to making decisions on security expenditures, the key to accountability is close consultation among the security specialists and the users, *with a documentation of the requirements and decisions based on mature risk management.* With this consultation and with the proper paper trail, it will be clear in any circumstance who is accountable for decisions and expenditures.

Considerable work will have to be done to ensure a closer working relationship with the geographic bureaux who manage missions abroad, and with the Physical Resources Bureau to ensure timely input of security considerations in the planning of mission projects. This two-way communication and cooperation should enhance respect for the integrity of security systems and procedures required by the department.

It must be stressed that security decisions at any level and in any location must be made on the basis of an informed threat and risk assessment and in accord with the Government Security Policy (GSP) which the Deputy is bound to administer, not solely at the discretion of the manager in place at the time.

Key Recommendation 1
***

Key Rec. 1. Response: Geographic bureaux, ADMs and their supporting Heads of Mission are responsible for implementing policy and making decisions on programs, staffing and budgeting at missions, and for determining what resources may be required to support these programs. With the exception of centrally-managed corporate systems, it is the responsibility of geographics to ensure that missions are adequately funded to maintain security systems, personnel and equipment required to protect assets, classified information and personnel against identified threats (on the basis of mature risk management) and in accord with corporate standards.

This recommendation was discussed extensively with geographic Area Management Advisors (AMAs). They were reluctant to take on operational responsibility and accountability for security-related decisions and expenditures because they considered that they did not have the necessary expertise to make security decisions. Even with advice from the Physical Security and Personal Safety Division (ISR), they might still be required to choose between conflicting priorities, for which they did not consider themselves to be well-equipped. Of equal importance was the question of funding security capital expenditures at missions. With a small capital budget centralized in ISR, as is now the case, funds can be allocated from time to time where they are most needed anywhere in the world. If the central budget were to be divided amongst the three geographic AMAs, it would be difficult to allocate funds, and shift them if necessary, in the most effective manner.

Key Recommendation 2
*Confirm that the Security and Intelligence Bureau (ISD) is responsible for developing corporate security policy in a changing global environment, ***, and for monitoring security activities, but that it does not retain any operating responsibilities or associated funds which would tend to violate the "user pay" process, except for funding inventories. (Supporting Recommendations are in italics below, before each response).*

Key Rec. 2. Response: Agree with the definition of responsibilities. The Bureau must retain funding and responsibility for some aspects of security operations (see the matrix in Annex I) to ensure corporate standards as well as a departmental capacity to respond quickly to emerging security and safety situations not anticipated in mission budgeting.

2.1 Invoke user pays concept for expenditures including life cycle that are requested or required by HQ program divisions and Missions.

2.1 "User pay" is already largely operative in the case of mission local security guards (not CBS Military Security Guards), and chancery and housing maintenance. Depending on the level of technology in question, "secure communications terminals" may be the responsibility of SXD or the mission.

2.2 Hold ISD accountable for security policy and standards, monitoring policy application, generating options for security safeguards, documenting buy-in and sign off of security options by geographics and missions.

2.2 Agree with all points. The AMAs and SRD agreed that an effective means of achieving a good level of consultation and buy-in would be the establishment and regular meeting of a sort of "security expenditure control committee". ISD will develop a plan for the formation of such a committee, and will in addition intensify its efforts to consult with other functional and geographic bureaux on security issues.

*2.3 ISD to develop and conduct revised approach to threat and risk assessments which include program managers involvement for program, support systems and site-*specific assessments and for the development of cost-effective risk-management solutions.

2.3 Agree. This is current practice, although the procedures are being improved. A standard and simplified template for mission Threat and Risk Assessments (TRA) has been developed, and will be used by *** to prepare an up-to-date TRA when a mission is inspected. TRAs will also be prepared to respond to special needs, such as the construction or renovation of a mission or when local conditions at a mission change materially. A key element of this process will be consultation with geographics and OGDs to ensure that we are working with an agreed TRA. That document will become the working document against which security decisions may be addressed.

2.4 Establish forum of program interests to discuss security issues.

2.4 Agree in principle. Meetings chaired by ISD will be held regularly with OGDs to discuss security-related issues.

2.5 Create service standards for ISD's corporate security support activities.

2.5 Security standards and service standards already exist but perhaps are not entirely understood by, or readily accessible to, all users. Security awareness and education programs can be intensified (more frequent briefings) to ensure all personnel are aware of security policy and standards and their own responsibilities in this regard.

2.6 ISD to develop compendium of best practices.

2.6 While recognizing the desirability of a published "compendium," resources are not currently available to embark on such an exercise until completion of work on the revision and update the manuals of security manual instructions. The concept of "best practices" is built into the work and thinking of the bureau.

2.7 Management accountability frameworks developed and implemented for ongoing security related decision making processes.

2.7 Management accountability frameworks exist for these functions, but are possibly not enforced as rigorously as they might be. In many situations, human resource limitations have resulted in apparent lapses. It is the intention of the ISD Bureau to assist other units in the accountability process for security management through more regular consultations, feedback and security awareness and education initiatives.

2.8 Provide Missions funds for Military Security Guard salary and allowance costs with ISD in a functional role or provide ISD funds and full responsibility and accountability.

2.8 We disagree that this responsibility should be an either/or decision. The Military Security Guard (MSG) program works extremely well as it is currently designed, as a centrally managed corporate resource with mission buy-in assured by the need to budget for local expenses.

The Military Security Guard (MSG) program is managed under an MOU with the Department of National Defence. Under this MOU an agreed number of military police are detached to DFAIT for assignment to missions abroad, where they act as mission security managers and guards. The MOU is administered by ISR. All salary costs, allowances, training, relocation and associated costs are paid by DND and reimbursed by ISR through ISDF.

Deployment of MSGs to missions is made at the request of geographic bureaux and missions, with the concurrence of ISR and based on agreed TRAs. Missions are responsible for local housing costs and any local operational costs such as travel within territory.

It is evident that there must be a central management of the MOU. It should be equally evident that a headquarters division is not in the best position to manage local housing of MSGs, but that the respective missions are. This shared responsibility is parallel to the management of the department's rotational personnel - assignments and salaries are managed at headquarters; the missions are responsible for paying local housing costs and local administration.

2.9 ISD to maintain inventory of security equipment which may be necessary to meet critical need. Missions to be responsible for cost of items.

2.9 Agree in principle. Much of the inventory provided to missions is already charged to mission budgets. In line with the approach in Annex I, we shall seek to implement a more rigorous charge-back system for security equipment for which missions are responsible. A period of experience will also be required to determine the financial requirements of maintaining an active inventory even with a charge-back system.

2.10 Funding for operating costs of armoured vehicles to be assigned to geographics and missions.

2.10 Agree. This is already standard operating procedure (see Annex I). ISR/ISDF has recently completed a review of requirements, maintenance schedules, and the divisions of fiscal responsibilities with missions whither armoured vehicles have been deployed. Vehicles will be assigned to missions only on the basis of agreed TRAs, and missions will be accountable for the proper maintenance and operation of the vehicles so long as they are required.

2.11 Establish purchasing and asset distribution framework. Implement charge-out process.

2.11 This is related to recommendation 2.9.

Possibly a basic conceptual flaw exists in insisting that missions be responsible for all such expenditures. In most cases when the need to make expenditures on security installations or equipment arises, it is the result of unforeseen incidents or the result of recommendations following a security inspection. Missions are not in a position to anticipate and plan for such expenditures, and therefore expeditious action would be hampered by lack of funds. AMAs have made it clear that they appreciate the ability of ISD to fund relatively small capital purchases or installations when the need arises. As always, the key to accountability is to ensure that both the responsible division (ISR) and the user (mission) agree on and have documented the need for any expenditure.

2.12 Define ISD's accountability for property security hardware and equipment and related funding.

2.12 A beginning has been made in the matrix in Annex 1.

2.13 Confirm ISD's role as purchasers, warehousers, and suppliers. Ensure that user requirements are paid by unit/mission involved.

2.13 Agree.

2.14 Consolidate HQ management of personal safety radios to maximize service capability while minimizing costs.

2.14 In the past, personal safety radio networks (PSRN) have been recommended or approved and funded by ISR, and installed in cooperation with SXT ***. This may change under the proposed matrix in Annex I. PSRNs should not to be confused with radio networks that missions may use for administrative or consular purposes and which are outside the scope of ISD. This issue is the subject of consultations with SXT, following which ISD will define precisely the responsibility for acquisition and maintenance of such systems.

***

Key Recommendation 4
Confirm that while the Physical Resources Bureau (SRD) is accountable for major chancery leasing and construction management, the Geographic and Program bureaux or OGDs as applicable, are responsible for formal sign off of SRD funding required to meet Program and Mission requirements. This is required to ensure that not only minimum facilities configurations based on ISD standards are implemeneted, but also that any special program needs are duly authorized. (Supporting Recommendations are in italics below, before each response)

Key Rec 4. Response: Agree.

4.1 Assign accountability for decisions impacting on security requirements to those whose operational decisions drive the security requirements.

4.1 Agree. Decisions shall be made against agreed TRAs and in accord with established departmental standards.

4.2 Assign funding responsibilities for mission property security safeguards to either the mission, SRD or ISD. Ensure separate funding responsibilities for corporate-wide security initiatives from ongoing security maintenance responsibilities, both at HQ and for missions.

4.2 For any new project, security features and installations (including IDACS) identified as required at the mission by the relevant geographic bureau, based on agreed TRAs, the advice of ISD and in accord with established departmental standards, should be funded by the project.

4.3 Match accountability for property security safeguards with funding authorities, ensuring that the recipients of the hardware concur with the safeguard choices made.

4.3 Safeguard choices shall be made based on agreed TRAs, the advice of ISD and in accord with established departmental standards.

4.4 Develop accounting policies for property security equipment and hardware that meet future requirements of accrual accounting and comptrollership.

4.4 SMSP is writing a general capital asset policy for the whole department taking into account the specific requirements of ISD and other bureaux with major responsibilities for material acquisitions and management. This bureau will continue its close liaison with SMSP on the development of this policy.

Key Recommendation 5
Institute mandatory security awareness and training programs for all staff at HQ and Missions. Require periodic competency testing for specified positions. (Supporting Recommendations are in italics below, before each response.)

Key Rec 5 Response: Agree. This is an ongoing project.

5.1 Expand coverage and content of ISDT security awareness and training programs. Require attendance for specified positions. Focus training on security safeguard responsibilities and accountability.

5.1 An expansion of the security awareness and education program has been incorporated into the coming year's business plan, including the allocation of additional resources. Specific projects are designed to address education gaps (many of which have been identified in this response). Priority is being given to security education programs which will be in line with CFSI's LES Training Strategy.

5.2 Conduct competency testing of positions responsible for specific security functions and cleared CBS.

5.2 ISD will review procedures to determine where or in what positions competency testing may be required. In general, *** are selected from the ranks of serving foreign service personnel who have demonstrated basic competencies.

Follow-up Action

The Security and Intelligence Bureau (ISD) has undertaken rounds of consultations with other bureaux to discuss, review and, where appropriate, modify security management practices in line with recommendations of the security audit.

Following is an outline of actions that have or will be taken to maintain this process and to ensure that accountability for security decisions is incorporated into business:

1 ISD has consulted with other functional bureaux mentioned in the audit (SRD and SXD) to ensure an understanding on the allocation of responsibilities in Annex I.

2. The ISD branch convened a meeting of geographic bureaux Area Managers to discuss budget and planning implications of enhanced responsibility for security, and efforts to enhance buy-in on security at the mission level.

3. In accord with recommendations of these AMAs and SRD, ISD will set up a process called "security expenditure review" consisting of regular meetings with AMAs and SRD and other interested parties to discuss security issues and major expenditure plans on security. In addition, ISD will seek to participate in regular planning sessions by the Physical Resources Bureau (SRD) to enhance planning and incorporation of security concerns in project planning.

4. ISR will enhance its consultation and collaboration with geographic bureaux, OGDs and intelligence sources to review, update and approve mission TRAs. This will be in the nature of a revolving (in terms of membership) TRA committee. ISR has also undertaken to revise and draft at least 30 mission TRAs per year, and this process is well under way.

5. ISD will seek to define and formalize the system of charge-back for the provision of security materiel to missions.

6. ISD will review the documentation on physical, personnel and IT security standards to ensure that they are easily accessible to concerned responsibility centres.

7. ISD will consult further with SXD on the variety of issues regarding the security of IT systems, personal safety radio systems and other communications issues to ensure that respective roles and responsibilities for information security are understood, and that adequate standards are in place and are respected. The Departmental Security Officer and the Chief Information Officer have undertaken to meet quarterly to review issues of mutual interest.

8. ISD will review accounting policies to ensure they comply with future requirements of accrual accounting and comptrollership.

ISD will expand its security awareness and training programs to respond to needs identified in the security audit, as well as ensure that an optimal segment of departmental employees have the necessary basis in security education to meet their responsibility for security according to their positions and duties.

ANNEX I

Security Decision-making and Funding Centres

10/12/1999

	Responsibility Centre
Headquarters Security	
All building and personnel security management at headquarters (the L.B. Pearson Building and facilities in the National Capital Region) is the responsibility of ISRG. They are responsible for providing protective services, administering the Commissionaire program, managing building safety and security, and identifying special security equipment for purchase as required. ISRG also manages the fire safety program for DFAIT in the NCR.	ISRG
PWGSC provides the building according to standards laid out in the Government Security Policy and special requirements of the department.	PWGSC
Mission Security	
The security of missions outside Canada is a joint responsibility of the Security and Intelligence Bureau (ISD), the geographic bureaux and the missions themselves, with specific security features as described below being the responsibility of other bureaux in the department	
1. Regional Security management and inspections ISD is responsible for maintaining departmental competence and policy in the application of GSP policies and requirements at missions.	ISR
*** ISR coordinates the preparation and adoption of Threat and Risk Assessments (TRA) for each mission in collaboration with the geographic bureaux, CSIS, OGDs and any other bureaux in the department involved in aspects of security.	
*** advises on security protective measures that should be put in place at missions, based on departmental standards and policies and relevant TRAs.	
*** conducts inspections of missions regularly to assist in the application of policies and standards and security measures, review TRAs, and provide advice to the Mission Security Officer.	

Geographic bureaux implement the policy decisions of Ministers, and decide where missions will be located, the programs that missions will deliver, the staffing requirements, budget levels and communications facilities. The missions (with reference levels from the geographics) are responsible for all local personnel (e.g. local guards) maintenance and support costs, and new installations and upgrades of security measures. When deciding on programs, systems and levels of personnel, budgets will take into account the application of any relevant departmental standards.	Geographics/ Missions
ISD through its *** coordinates and promulgates policy for the support of security systems, protection of property and personnel, physical installations and the protection and integrity of commendations systems.	***
2. Threat and Risk Assessments	
Mission specific TRAs will be prepared by ISR and will be reviewed and accepted by the relevant geographic bureau. Subsequent decisions in respect of security requirements will be made with reference to the agreed threats and acceptable risks, and in accord with applicable departmental standards.	ISR/ Geographics
Project or item-specific TRAs on physical security will be prepared by missions and approved by ISR for any significant new expenditures whether by missions or by headquarters in response to security and safety threats.	Missions/ ISR
3. Armoured Vehicles	***
ISD through a working group from ***, and with the technical support of the RCMP under an MOU, manage the department's fleet of armoured vehicles through its life cycle. Vehicles are deployed to missions at the request of missions and based on agreed TRAs. ISR is responsible for funding the acquisition of vehicles, funding an inventory of specialized parts or for the replacement of specialized parts, the training of drivers and maintenance personnel as required and for the original shipping of a vehicle to a mission.	
Missions are responsible for the day-to-day operation and maintenance of the vehicle, including parts that are normally accessible at missions. Missions are responsible for the return transportation of vehicles when no longer required.	Missions

4. Military Security Guard Program — ISR, ISDF

The Military Security Guard (MSG) program is managed under an MOU with the Department of National Defence. Under this MOU an agreed number of military police are detached to DFAIT for assignment to missions abroad, where they act as mission security managers.

The MOU is administered by ISR. All salary costs, allowances, training, relocation and associated costs are paid by DND and reimbursed by ISR through ISDF.

Deployment of MSGs to missions are made at the request of geographic bureaux and missions, with the concurrence of ISR and based on agreed TRAs. — Geographics/ Missions/ ISR

Missions are responsible for local housing costs and any local operational costs such as travel within territory. — Missions

Travel outside mission territory undertaken at the request of ISR will be the responsibility of ISR or the mission requiring assistance depending on circumstances. — ISR

5. Chancery, Housing and Property Projects and Fit-ups

The Property Management Bureau (SRD) continues to be responsible for planning and financing all new property projects outside Canada (Key Recommendation 4). In drawing up plans, SRD responds to the requirements for size and program requirements from the geographics, and to security requirements from ISD (ISR and ISC). Security installations and requirements will be based on the agreed TRA, departmental standards in place and specific requirements for the protection of specific elements of sensitive or classified equipment which the "user" has identified as necessary for carrying out the programs of the mission. All project and fit-up costs should be calculated as part of a project budget. — SRD

6. Security Installations and Equipment at Missions — Missions

All security installations or equipment installed in a mission once an initial project has been commissioned, and the operation and maintenance of all such equipment, will be the responsibility of the mission. This may include the addition of BR windows and access control barriers, grills, alarms and safe havens at staff quarters. ISR will advise on corporate requirements and standards that will apply.

Missions should plan for the maintenance and replacement of security equipment installed in offices and staff quarters — Missions/ AMAs

Missions are also responsible for the provision of any personal safety equipment that may be required, based on TRAs and with the advice of the regional security managers in ISR.	Missions
In order to ensure ready availability to standard security equipment, such as locking devices, cabinets, shredders, ISDF will maintain an inventory of most standard equipment and will seek reimbursement from missions or headquarters divisions for equipment delivered.	ISDF
Provision has been made to allow ISR to fund newly-identified security installations and equipment whose need could not be readily foreseen in mission budget planning. Such expenditures may arise from emergency situations that arise at a mission, or installations that may be recommended as a result of a security inpsection.	ISR
7 Communications Security	
The Information Management Bureau (SXD) is responsible for the design, development and maintenance of secure corporate communications (Key Recommendation 3). This includes the telephone network, the computer-based electronic communications network, secure telephone systems and the personal safety radio networks (PSRN) at missions. SXD sets policies for the reimbursement by geographics and missions for the provision of these services.	SXD
Decisions regarding the deployment of various types of secure communications systems at missions are made the geographics in consultation with ISD and SXD based on program requirements and TRAs.	Geographics/ ISD/ SXD
ISD *** is responsible for *** the development of security plans and policies.	***
The accountability, control and distribution of *** both at HQ and Missions is managed by ISDF ***	ISDF
Headquarters maintains an inventory of ***. These may be sent to missions at the request of missions (and where missions can provide the required protection of equipment and information that may be processed), and will missions will be charged .	Missions
8. Mail and Courier Services	
The Distribution Services Division (SBG) provides Diplomatic Courier Services and the secure handling of designated and classified mail within the department, based on the requirements of the GSP and departmental security standards.	SBG
9. Technical Security	
***	***

10. Security Education, Training and Awareness

ISD through its Personnel Security and Education Unit (ISDT) provides briefings to staff on a range of security issues to prepare the department's employees to better understand and manage their responsibilities for the protection of designated and classified information, government assets and the personal safety of staff and CBS dependents at missions. This unit also provides a range of information related to these issues.	ISDT

11. Personnel Security

***	***

12. Intelligence Liaison Services

***	***
***	***