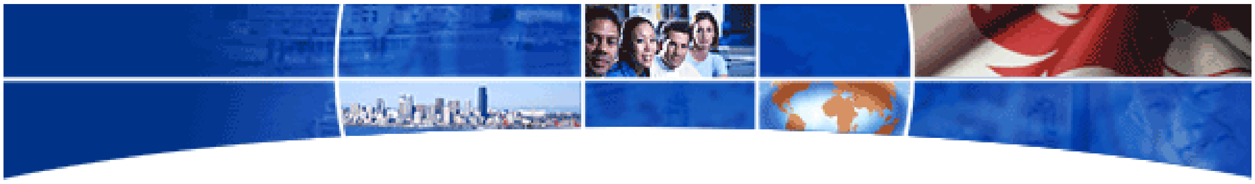


FINAL REPORT

AUDIT OF

DFAIT CONNECTIVITY TO THE INTERNET

March 29, 2004

Departments of Foreign Affairs and International Trade
Office of the Inspector General
Audit Division (SIV)

TABLE OF CONTENTS

APPENDICES

EXECUTIVE SUMMARY

Background

As part of the Audit Division's ongoing discussions with DFAIT management on risk monitoring activities in DFAIT, SIV solicited input from Departmental staff on key issues related to DFAIT's connectivity to the Internet. Resulting from these discussions, the following audit was conducted as part of the audit plan for 2002 - 2003. (SIV undertook an earlier audit in 1998 which covered the internal Intranet, Departmental Web sites, firewalls and router service provided to DFAIT by PWGSC.)

At Headquarters, the audit included focus groups to rank significant risk factors related to Internet operations and since Internet access is provided to all staff, 10 Missions were also included in the audit coverage. Where possible, benchmarking was undertaken to establish a comparison of DFAIT against identified "Best Practices" from other government departments and the private sector.

Key Findings

Since 1998 DFAIT has continued to experience growth in the available content of its Web sites and in the amount of internet usage by staff and clients. The number of Departmental Web sites has now stabilised over the previous period and a structure for governance has been established. As such, the Department has made progress since 1998 to establish a comprehensive management framework to support these activities.

We expect a continuing demand for Web enabled solutions in applications, mobile and wireless computing, program service delivery, public participation in policy formulation and in electronic commerce. These demands will challenge DFAIT's capability to ensure that the required security and privacy components are built into the planning and design of these initiatives. Demonstrated support by senior management through the provision of appropriate levels of resourcing for the security components of these initiatives will be required.

The Department has not yet established a comprehensive costing model for these activities. In particular, the audit identified that there is no identified process for capturing and reporting on an ongoing basis the total Internet-related costs to the Department. This means that management's ability to substantiate and allocate resources among competing corporate priorities has a less than optimal rationale to support the decisions taken. The audit recommends that DFAIT undertake a costing exercise to integrate financial accounting concepts into the strategic monitoring and reporting of IT costs to senior management.

The audit identified several areas where the management framework to support the provision of privacy and other aspects of the Department's Web presence would require additional focus by management with respect to new requirements related to the Privacy Act.

The Treasury Board Secretariat has recently issued a document entitled the "Security Domain Architecture" for the GoC. All Departments are expected over a three-year time frame to consider and incorporate the security domain concepts and IT Security Zones introduced in the document into their specific environments. The document is under review in DFAIT and it is expected that various components of the framework will be integrated into the planning and development activities for the Departmental network and applications.

The report identifies opportunities to increase staff awareness of available Departmental training and also notes areas of improvement which have emerged since the previous audit. For example, the growing relevance of the Internet Operations Committee (IOC) and new requirements for business case analysis for new Web sites is encouraging. A business case must now be presented for any new Internet connectivity or Web service proposed within DFAIT. In addition, the Department has recently procured software tools which, when implemented, will allow enhanced content management of Departmental Web sites.

OBJECTIVES AND SCOPE

The objectives of the audit were to assess:

- the efficiency and effectiveness of the Internet implementation in meeting user requirements and achieving stated objectives;
- the adequacy of, and compliance with policies, procedures and operational controls by users of the Internet;
- the adequacy of staff training (i.e., DFAIT end-users and technical support staff);
- whether standards and policies for confidentiality[1], availability[2] and integrity[3] are being met; and,
- whether the Departmental firewalls are adequately administered.

The growing reliance by the public on the Internet to provide up-to-the-minute information is leading Web content providers to consider their operations in the context of high-availability 7/24 operations. Similarly, DFAIT's Interim Business Continuity Plan lists Internet operations as critical; therefore the audit team reviewed the current status of the Interim Departmental Business Continuity Plan (BCP)[4,5].

The BCP states that "*as the Internet would constitute a critical tool for communicating essential information to the public and instructions to employees, it will be essential to restore a basic Internet presence, even if rudimentary*." Though it was beyond the scope of this audit to review the entire plan, the plan generally appears sound in its start-up approach, pending completion of all sections of the plan. Overall, the audit team is of the opinion that, subject to completing a full drill of the BCP and incorporating any lessons learned, the Department has made progress with the development of the interim BCP.

As identified in the Terms of Reference, the audit included components of Signet-O[6] such as the DNS servers and mail server gateways (i.e., SMTP, X.400, excluding Web servers specific to Government On-Line). At the time of the audit, Departmental firewalls isolated Signet-O from the Signet-DMZ, the Signet-OGD network and Signet-D. These network areas were included within the scope of the audit. Signet Remote Access and services were excluded from the audit.

[1] Confidentiality - "the sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of injury should unauthorized disclosure occur", **Audit Guide - Information Technology Security,** Treasury Board Secretariat, 1995.

[2] Availability - "the condition of being usable on demand to support business functions", **Audit Guide - Information Technology Security**, Treasury Board Secretariat, 1995.

[3] Integrity - "the accuracy and completeness of information and assets and the authenticity of transactions", **Audit Guide - Information Technology Security**, Treasury Board Secretariat, 1995.

[4] CANADA. Department of Foreign Affairs and International Trade. *Record of Executive Committee Meeting of January 9, 2002.* 19 March 2002. (http://intranet/department/executive/2002/020109-e.asp)

[5] CANADA. Department of Foreign Affairs and International Trade. *Interim Departmental Business Continuity Plan.* January 18, 2002.

[6] CANADA. Department of Foreign Affairs and International Trade. *Intrusion Detection Implementation Review*, SXIA, March 30, 2001

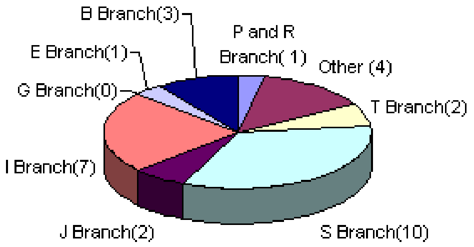
PHASES

Risk Ranking

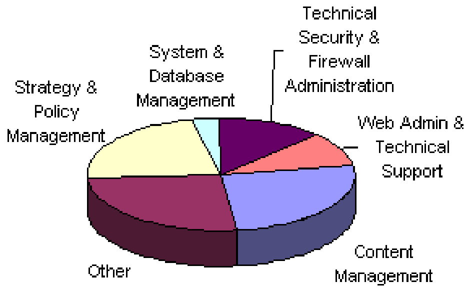
The first phase of the audit included an assessment and ranking of risk factors related to DFAIT's connectivity to the Internet, as well as ongoing plans for development of alternative Internet-based service delivery mechanisms. Risk areas were identified and considered in relation to the risk of failure to meet the Departmental objectives, and the risk of failure to safeguard Departmental assets. The items identified were ranked in order of importance, with the key items forming the focus of the second phase of the audit.

The issues were identified through the use of focus groups. The focus groups were asked to rank the issues according to impact (to the Department), and likeliness to occur (or risk). The focus groups consisted of a cross-section of individuals from the Department (see **Appendix C**) involved in Internet operations and services, security, and program delivery. The following charts illustrate the representation of the various branches, as well as the roles of the individuals who participated.

Focus Group Representation by Branch



Roles and Responsibilities of Participants



Risks may be either internal or external. Internal risks are mostly operational in nature and can usually be controlled by managers, while external risks are more strategic in nature and typically involve factors beyond a manager's direct control. The risk ranking includes an analysis of all identified risks, both internal and external, to determine the likelihood that events which can compromise the Department could occur, and the potential negative effects or impacts that a given event could have. This analysis relied heavily on the experience, insight and operational perspective of focus group participants.

Field Work

After the completion of the risk ranking the audit field work was initiated. The following list of activities provides an overview of the tasks that were undertaken:

- Ensure that the Department has processes to ensure that the most current version of all software and patches are implemented on the firewalls and Web servers.
- Review and evaluate all password account management procedures.
- Review and evaluate processes for event handling of all logs produced by the firewalls and Web servers.
- Review and evaluate access rights to the files and directories on the firewalls and Web servers.
- Ensure that processes exist to disable all commands posing a security risk or are enabled for only appropriate authorized accounts.
- Review and evaluate removable media storage/retention and inventory procedures.
- Review and evaluate software change procedures for the firewalls and Web servers.
- Assess physical security of firewalls and Web servers.
- Review and evaluate virus detection and control procedures.
- Review and evaluate procedures for changing rules on the firewalls.
- Review and evaluate processes to enforce firewall rules.
- Review and evaluate procedures for backup of firewalls and Web servers.
- Review Internet business process issues and overall direction of Departmental Internet activities.
- Gather information on Best Practices and Benchmarking at other Departments, and the private sector.

Appendix B provides a list of the participants by organizational unit which were interviewed.

Benchmarking and Best Practices

Benchmarking compares an organization's performance "*to that of world-class organizations in order to measure business excellence and establish realistic goals for improvement. ... Benchmarking is a performance measure that provides the driving force to establish goals of high performance and the means to accomplish these goals*."[7]

In order to evaluate best practices of other government departments and private sector companies of similar size and mandate, the team interviewed staff at Public Works and Government Services Canada (PWGSC), Department of National Defence (DND), and Human Resources Development Canada (HRDC).

The team utilized information from Gillette Corporation and IBM Corporation and also researched European and U.S. Government publications, particularly those of the U.S. General Accounting Office (GAO) and National Institute of Standards and Technology (NIST). Where

[7] *Implementing Benchmarking*, August 1999, CMA Canada.

applicable, relevant, and current, Treasury Board Secretariat policies and publications, including RCMP and CSE technical standards and guides were utilized.

DETAILED FINDINGS

1. Cost Recognition and Reporting

1.1 Total Cost of Ownership

The issue of transparency of Internet-related costs is problematic in DFAIT as there is no identified process for capturing and reporting on an ongoing basis the total costs to the Department. This means that management's ability to substantiate and allocate resources among competing corporate priorities has a less than optimal rationale to support the decisions taken.

No one could direct the audit team to a report, budget item, or accounting practice that could be used to determine what Internet connectivity and Web presence is costing the Department. Audit interviews indicate that there had been a previous report that gave a "cost-per-head" of Internet connectivity, but we were unable to locate the report and had insufficient information to determine what costs were included in the report to arrive at this calculation. Several discussions indicated that the costs included were primarily hardware and telecommunications leased lines ("bandwidth"). Indirect costs including apportioned software, Web management, programming personnel, and other intangible costs were not included.

> "*Determining costs is essential for good management of programs and services. It is needed for determining user charges, for informed allocation of resources among service delivery components, and for decision-making that is based on affordability. ... Roles and responsibilities: Departments are responsible for establishing service standards and informing their clients of service standards, including the costs of delivering the services. Service delivery managers are expected to take the lead in this development. Departmental financial services are expected to be able to advise managers on practical and accurate ways of determining relevant costs of service delivery.*"[8]

It is no longer good enough for managers to just spend money on IT without being able to demonstrate the magnitude and tangible benefits of those expenses. Total Cost of Ownership (TCO) is a method to iteratively calculate and refine both sides of that equation.

An approved policy document posted on the CIO/IMT Policy Web site defines TCO as: "*Total Cost of Ownership: For an IMT system, application or resource, this is the sum of the initial capital (project-related) costs and both direct and indirect costs of operation for the lesser of the first five years of operation or its expected useful life span*."[9] The document does explain that project managers must have that calculation available in order to decide whether they need Departmental approval for their IM/IT project. However, there is no explanation as to how to calculate the total costs or where that information is available.

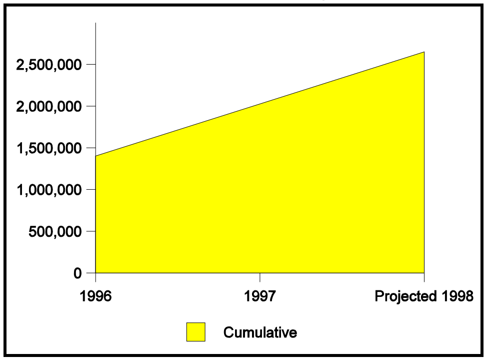
[8] CANADA. Treasury Board Secretariat of Canada. *A Guide to Costing of Service Delivery for Service Standards*. October, 1995.

[9] CANADA. Department of Foreign Affairs and International Trade. *Policy on Approvals Process for Proposed Information Management and Technology Projects*. Posted on the CIO/IMT Intranet Web site at http://intranet/department/cio/proManagement/tracking/policyProcess-e.asp

In January 1999, a Gartner Group Total Cost of Ownership modelling package was purchased by SXD, with the approval of the IMT Steering Committee, and an initial TCO exercise conducted. This first iteration was primarily focussed on TCO of the help desk and user support function. Much work was applied to gather the data and define it in terms consistent with the Gartner Group model. That exercise represents much effort and good work on the part of those concerned. Subsequent periodic (annually or better) TCO calculations could build on this foundation.

As another example of how achievable the initial TCO calculation would be, a cumulative estimate of the Internet connectivity costs was provided in the previous 1998 audit. In 1998 these costs represented $2.5 million per annum. The report also noted that, "*These costs exclude the current cost of development for various mission Home Pages, which are not identified, consolidated and reported at Headquarters. In short, the chart understates the true cost of this activity to the department..*"[10] The chart depicts a cost clearly on the rise over time and which in our view warrants monitoring and analysis.

Internet Connectivity Costs



Defensible determination of the TCO for Internet connectivity and Web presence would reinforce the mandate of the CIO, contribute to the required Departmental implementation of the TBS Modern Comptrollership Initiative and Enhanced Management Framework (EMF), and integrate with the general thrust of the GoC Financial Implementation Strategy (FIS), which is to provide more accurate reporting. The benefits derived by integrating financial accounting concepts into strategic monitoring of IT costs was described in a PWGSC report which stated that " *'We can measure how we consume things rather than just how we spend money.' ... The improved quality of the financial information being disseminated to departments and agencies will result in better decision-making, planning, and reporting.*"[11]

Because the Department already has experience with the Gartner Group program, which is a recognized and credible model, application of the model to the TCO of Internet connectivity and

[10] CANADA. Department of Foreign Affairs and International Trade. *Audit Report on DFAIT Connectivity to the Internet*. June 19, 1998.

[11] CANADA. Public Works and Government Services Canada (PWGSC). *Doing Business with Public Works and Government Services Canada, 'FIS: a smooth transition to new-and-improved accounting method.'* Spring 2002. Single quoted portion attributed to Rod Monette, Assistant Deputy Minister , Government Operational Services (GOS).

Web presence might yield more immediate results than would be expected on an untried first iteration. Subsequent iterations could be used to refine the results.

Ultimately, the decisions taken with respect to informatics expenditures will benefit from an approach which allocates measured costs against competing business requirements and priorities. Without a method to budget and account for total Internet connectivity and Web presence, it is difficult to ascertain whether the expenditures are achieving expected benefits.

Interviews conducted during the audit indicate that a range of disparate budgeting practices exist across the Department for Internet connectivity. For example, the long-range Internet connectivity plans are being developed in concert with the Government On-Line initiative. The general IT budget is determined departmentally, but the criteria for budgeting for Internet connectivity, including Web site development and maintenance are short-range and appear to be local to the bureau or division.

Recommendation(s):

- **The CIO, in consultation with SMD/SAM, should undertake an exercise to determine the Total Costs for Departmental Internet connectivity and Web presence, and ensure the process is maintained on an ongoing basis as an annual budget item.**

Management Action:

CIO Response:

The CIO will undertake in 2004/5 a departmental wide review of all IM and IT expenditures and will report the findings to Executive Committee. This will include an assessment of the total cost of departmental Internet connectivity.

ISC Comments:

ISC's resources are being utilised during investigations that include monitoring and accessing logs related to an individual's Internet activity. The recommendation related to determining the "Total Costs for Departmental Internet connectivity" which would show the "cost/benefit" would be welcomed and supported by our bureau.

DCP Comments:

DCP resources are similarly utilized in order to meet ongoing departmental and central agency requirements related to the provision of privacy on new applications, including those delivered over the Internet. The recommendation related to determining the "Total Costs for Departmental Internet connectivity" which would capture and report on these costs would be welcomed and supported by our bureau.

1.2 Cost/Benefit Monitoring

The Cost/Benefit Monitoring Process specific to Internet Connectivity and Web Presence is not evident within DFAIT. As a result, management cannot be assured that Internet expenses are efficiently and effectively meeting DFAIT's needs.

As with budgeting, a companion method of addressing management's problem in allocating scarce resources is comparing the expected benefits of an investment to the costs. For very large investments an Economic Feasibility Study determines whether the projected expenditure is warranted, affordable, and if alternatives might be available.

Cost/Benefit Justification, or a Business Case requirement, is a management control to guarantee that the delivery of services by the Internet function is cost justified and in line with the industry.

The Departmental CIO/IMT *Policy on Approvals Process for Proposed Information Management and Technology Projects* requires that any project whose estimated total cost of ownership (capital plus five-year operation) exceeds $200,000, or whose risk and/or impact is judged to be medium or high shall be subject to Departmental approval.

A cost monitoring process that compares actuals to budgets is performed as part of the annual overall Departmental accounting process and as with budgeting, the audit team was not able to identify a cost monitoring process specific to Internet connectivity. IT budgeting appears to be concentrated on hardware, software licensing, and bandwidth whereas related soft costs (e.g. Web development, Web surfing, etc.) are not tracked or analyzed for Cost/Benefit.

The growing relevance of the Internet Operations Committee (IOC) and its demands for business case analysis for new Web sites is encouraging. A business case must be presented for any new Internet connectivity or Web service proposed within DFAIT. However the audit team could not identify whether there is a current requirement to regularly review existing Internet connectivity and Web presence Business Cases for continuing relevance.

Management does not call out specific Internet connectivity and Web presence costs in the budgeting process and no financial metrics have been developed to assess the effectiveness of the Department's Internet connectivity or Web presence. There appears to be no document available that links the cost of Internet connectivity and Web presence expenditures with the achievement of overall Departmental Information Management strategies and desired outcomes. Management's identified goals for Internet connectivity and Web presence are not specific enough to determine the extent to which planned objectives have been achieved, deliverables obtained, performance targets met, and risks mitigated.

Best Practice(s):

A formal System Development Life Cycle (SDLC) methodology is adopted. It requires, in each proposed information systems development, implementation, and modification project, an analysis of the costs and benefits associated with each alternative being considered for satisfying the established business requirements, including a complete Economic Feasibility Study for major projects.

Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Upon review, appropriate management action should be initiated and controlled.

Recommendation(s):

- **The CIO, in consultation with SMD/SAM, should develop a Departmental Internet Connectivity and Web presence cost/benefit monitoring process and apply it across DFAIT.**

Management Action:

CIO Response:

The departmental wide review of all IM and IT expenditures referred to in 1.1 will also lead to the development of a cost/benefit monitoring process applicable across the department.

2. Privacy Act

2.1 DFAIT's adherence to the requirements of the Privacy Act has not been assured on all Web sites. This could lead to Departmental embarrassment or liability should personal information be disclosed in an unauthorized manner.

The Privacy Act protects the privacy of personal information held by a government institution. DFAIT is bound by its requirement to limit personal information collected, to protect its disclosure, and to ensure that the information is only used for the purposes for which it is collected.

DFAIT has adopted a Departmental policy that requires notification to Web site visitors of any personal information that the Department will capture. For the Web pages viewed by the audit team, the privacy statement was evident. (Refer to "*Important Notices - Government of Canada Privacy Statement*" from the DFAIT Home page.) The Department generally limits its collection of information to the IP address of visitors for statistical purposes. Privacy Impact Assessments (PIA) are now required for all government of Canada information systems that may potentially collect personal information.

However, on the Team Canada e-XACT site, personal information is being collected from the public, including credit card numbers for a specific application, and may not be sufficiently protected. No Privacy Impact Assessment was produced for this application nor was a Threat and Risk Assessment (TRA) performed on the system prior to the site's development and subsequent operation. (The project was in pilot mode in London and New York during the period in which the audit was conducted.)

Best Practice(s):

Best practice organizations perform Privacy Impact Assessments (PIA) on all extant systems and make a PIA required as part of new system development. (As well, PIA recommendations must be addressed prior to accreditation or re-accreditation of IS.)

Recommendation(s):

- **If it is intended to proceed further from pilot to implementation, SMF and ISC in consultation with PWGSC should conduct a TRA on the e-XACT application.**

- **DCP should be contacted by SMF for guidance on the requirement of a Privacy Impact Assessment (PIA) on the e-XACT application.**

Management Action:

SMF Response:

The e-XACT pilot was abandoned due to the lack of flexibility with the product. We are now looking at the "buy button" product of PWGSC. SMF will initiate discussions with ISC to ensure the actions requested in the recommendation are taken on the "buy button" product as well.

ISC Response:

The Departmental responsibility associated with the collection of personal information including credit card numbers is an issue of concern. The department has an obligation to protect this information and recent cases in other departments where this information has not been safeguarded as it should have been, has made headlines in the media. Regarding the specific recommendation related to the Team Canada e-XACT site, we understand that this application was not implemented and therefore no TRA was performed. ISC will however follow-up with SMF and PWGSC to see if another application was implemented in its place.

3. User Training

3.1 DFAIT users lack awareness of available Internet-related training. This may contribute to user dissatisfaction with supplied desktop tools, reduced operational efficiency in training services, and productivity losses for DFAIT.

Although the Canadian Foreign Service Institute (CFSI) maintains a range of training offerings as well as baseline curriculum of "course lists" by employee position and category,[12,13] focus group participants indicated that training relating to Internet was limited or not available.

In the area of Internet development and management, CFSI demonstrated to the team how, in addition to courses already on offer, they coordinate the provision of training from external training organizations where cost/benefits analysis does not justify the development of an in-house training program. Training statistics indicate that the number of cancellations is 31%, and the number of no-shows is 29%. CFSI indicated that it is up to the employee and their manager to review the training needs and request suitable training. CFSI also indicated that they pursue alternative delivery methods, such as distance learning and network learning, in order to provide employees throughout DFAIT with a range of options suiting their needs. These approaches also enable CFSI to deliver training to any mission connected to the DFAIT network.

However, since portions of the sampled user population were unaware of the extensive training available from CFSI, they are not taking advantage of it. Untrained staff may not be optimizing their use of computing and Internet resources. The fact that extensive training packages are available, but the user population is unaware of them, indicates an opportunity to enhance staff awareness of available training.

Best Practices:

Best practices organizations maintain a training system that links Internet skills and proficiency levels to regularly reviewed and updated job descriptions. If incumbents lack skills or proficiencies, the requisite training is mandatory and is tracked by the personnel system and management. Incumbents are given every encouragement to acquire the necessary skills and proficiencies, but for cases where the incumbent fails to respond to those encouragements, a reasonable deadline for acquiring them is given that considers the intricacy of the skill or proficiency. Management is also given incentives to ensure that their people are well-trained and current.

Similarly, DFAIT HR (MSL/HPD/HRD) could ensure that Internet and IT skills and proficiencies are linked to all job descriptions, perhaps as part of the Competency-Based Human Resources Management Project. Acquisition of the skills and proficiencies should be mandatory, as evidenced by attendance on relevant CFSI courses or provision of other acceptable proof. Incumbents' possession and use of the requisite skills and proficiencies could then be identified and supported by the various personnel and training systems and management.

[12] CANADA. Department of Foreign Affairs and International Trade. *Positions and Employee Groups*. 7 May 2002 (http://intranetapps/cfsi/virtual/14EmployeeGroups/EmployeeGroups-e.asp)

[13] CANADA. Department of Foreign Affairs and International Trade. *Course: Internet and DFAIT Intranet.* 7 May 2002 (http://intranetapps/cfsi/virtual/11CFSIcourses/courseInfo-e.asp?id=100)

Recommendation(s):

- **The Canadian Foreign Service Institute (CFSI) should expand their training program to educate DFAIT staff on the wide range of Internet and IT training available from the Institute and the availability of outside training when appropriate.**

- **CFSS should focus on the needs of missions and should officially advertise its Remote Training Program to missions.**

Management Action:

CFSI/CFSS Response:

CFSI and CFSS agree in principle with the intent of the observations in the audit report. However, the question of long term funding would require additional resolution and concurrence of SXD. We will initiate a dialogue with SXE to examine the long-term funding issue.

The upcoming Infrastructure Renewal Project (IRP) will give us opportunities over the next two years to expand the IMT training program to include a wide range of Internet and IT Training available from outside of the Institute as well as increase its current list of on-line products and increase its use of Remote Training to deliver IMT workshops directly to missions from Ottawa.

CFSS has been working with SXD for the past months to utilize various pieces of educational technology that are either currently available or will be available when the Infrastructure Renewal Project takes place. Some of these pieces of educational technology are: an Authorware Web Player on each desktop, Remote Assistance Feature of XP, Impatica on Cue and an IMT Learning Portal which will be available to missions and headquarters.

These pieces of technology are all different from the perspective of how we can use them. Authorware Web Player will allow us to design and develop or buy CBTs which can be played off the departmental Intranet. The Remote Assistance feature of XP will allow us to link training/coaching directly to the desktop of the IMT user. Impatica on Cue will allow us to use MS PowerPoint in interactive on-line tutorials which are quick and easy to develop. The IMT Learning Portal will house the on-line products that have been and will continue to be developed in house, but it will also make it possible for CFSI to use Internet and IMT training packages that are currently available from outside sources. DFSS is currently publishing with SXM and Public Works a Request for Proposal to procure a bilingual library of IMT training packages which can be placed on the IMT Learning Portal. The timeframe for the IMT Learning Portal to be up and running is October/November 2003.

ISC Comments:

Although there is no specific recommendation related to the DSO, our NAUP investigations have shown a lack of awareness by many DFAIT employees on the content of the Network Acceptable Use Policy. In this context, we would recommend that the NAUP be handed out to all those attending "Internet" related training being conducted by CFSI.

APPENDICES
Focus Group Results

The results of the risk ranking exercise indicated that the top six issues in terms of impact and likeliness to occur are:

- Lack of training initiatives and staff development activities related to Internet management and implementation

- Not ensuring that processes are put in place to ensure that program back-ends can support the increase in traffic

- Not having a contingency and recovery plan

- Internet Strategy: Of not having clear service delivery linking DFAIT business objectives to Internet strategy

- Not having formal configuration and change procedures

- Lack of user awareness of procedures for virus protection

Participants

Position	Organization
Senior Connectivity Officer	REB, European Business Development and Connectivity Initiatives
Chief Information Officer and Director General	SXD, Information Management and Technology Bureau
Director, IMT Planning & Direction	SXP, IMT Planning and Direction Division
Director, Infrastructure management	SXT, Infrastructure Technology Division
Account Manager	SXCA, Account Management Section
A/Manager, Information Services	SXCI, Information Services
Client Interface, Intranet	SXC, Client Services Division
Manager, Internet Dev. & IOC	BCP, Outreach Programs and E-Communications Division
Connectivity Officer	REB, European Business Development and Connectivity Initiatives
Deputy Director & IOC observer	SXPL, IMT Planning and Policy Section
Webmaster	JPC, Informatics
Director, Information Resources	SXI, Information Resources Division
Project Content Manager (& IOC)	MJW, Assistant Deputy Minister (Portfolio: Global and Security Policy)
Director, Trade & IOC	TCW, Trade Commissioner Service Marketing Division
Deputy Director, Government on Line	SXG, Government On-Line Project Office
Deputy Director, Email and Gateways	SXTE, Mail and Gateways Section
Deputy Director, Secure Systems	SXTC, Secure Systems Section
Manager, Secure Systems Development	SXTC, Secure Systems Section
Strategist, Cybercommunications	BCP, Outreach Programs and E-Communications Division
Policy Co-ordinator IT Security	ISC, Corporate Security Division
Counsellor, Info Highway and Youth	IMF, Francophonie Affairs Division
Lead Internet Systems Administrator	SXIA, Information Availability
Program Coordinator, Outreach & Comm.	AGP, Peacebuilding and Human Security Division
Director, Centre for Corp. Learning	CFSS, Centre for Corporate Services Learning
Database Manager	TCE, Export Development Division
IT Security Analyst	ISC, Corporate Security Division
Officer (Web Administration, Technology Support)	NUR, United States General Relations Division
IM/IT Advisor & IOC observer	EAM, Area Management Office - Trade and Economic Policy
Deputy Director/ IT Security Specialist	ISC, Corporate Security Division

Risk Ranking Participants

Position	Organization
Manager, Internet Dev. & IOC	BCP
Communications Officer, Internet Dev.	BCP
Program Coordinator, Outreach & Comm.	ILX
Elections Coordinator	IMOP
TIP Co-ord. & Web Content Mgr (Communications Officer & IOC)	JPS
Internet Content Manager & IOC observer	PNSP
Counsellor, Info Highway and Youth	IMF
Director, Information Resources & IOC	SXI
Director, IMT Planning & Direction	SXP
Co-ordinator, CanadExports On-Line	PNSP
Dep. Director	GAF
IT Security Analyst	ISC
Client Interface, Intranet	SXC
Deputy Director & IOC observer	SXPL
Dep. Director, TCS Information Systems	TCE
Manager, Visits Program, REB	REB
IM/IT Advisor & IOC observer	EAM
Webmaster, Financial Management Off.	IDA
Policy Coordinator, IT Security	ISC
Project Content Manager (& IOC)	MJW
Web Admin & Tech Support N Branch	NUR
Manager, Secure Systems Development	SXTC
Webmaster	JPC
Database Manager	TCE
Education Marketing Unit	ACET
A/Manager, Information Services	SXCI
Director, Centre for Corp. Learning	CFSS
Deputy Director/ IT Security Specialist	ISC
Lead Internet Systems Administrator	SXIA
Dep. Director, Email and Gateways	SXIM
Deputy Director, Government on Line	SXG
Account Manager	SXCA
Deputy Director Secure Systems	SXTC
Strategist, Cybercommunications	BCP
Director, Trade & IOC	TCW

Glossary

[NB: This Glossary is taken from *Government Security Policy (2002)*.]

Accreditation *(accréditation)* - the official authorisation by management for the operation of an IT system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations.

Assets *(biens)* - tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation. (The inclusion of information in this definition is for the purposes of this policy only and should not be interpreted as importing any legal consequences applicable for assets to information.)

Availability (*disponibilité*) - the condition of being usable on demand to support operations, programs and services.

Baseline security requirements *(exigences sécuritaires de base)* - mandatory provisions of the Government Security Policy and its associated operational standards and technical documentation.

Business continuity planning (planification de la continuité opérationnelle - an all-encompassing term which includes the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets.

Certification *(certification)* - a comprehensive evaluation of the technical and non-technical security features of an IT system and other related safeguards to establish the extent to which a particular design and implementation meets a specific set of security requirements, made in support of the accreditation process.

Classified assets (*biens classifiés*) - assets whose unauthorized disclosure would reasonably be expected to cause injury to the national interest.

Classified information (*renseignements classifiés*) - information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest.

Compromise (*compromission*) - unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

***COMSEC* -** communications security: cryptographic, transmission and emission security measures applied to information stored, processed or transmitted electronically; a subset of information technology security.

Confidentiality (*confidentialité*) - the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the *Access to Information Act* and the *Privacy Act*.

Contracting process (p*rocessus de passation des marchés*) - includes bidding, negotiating, awarding, performance and termination of contracts.

Critical assets *(bien essentiels)* - assets supporting a critical service.

Critical service *(service critique*) - service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the efficient functioning of the Government of Canada.

Facility (*installation*) - a physical setting used to serve a specific purpose. A facility may be part of a building, a whole building, or a building plus its site; or it may be a construction that is not a building. The term encompasses both the physical object and its use.

For cause *(pour un motif valable)* - a determination that there is sufficient reason to review, revoke, suspend or downgrade a reliability status or a security clearance. In the context of a security assessment, a determination whether more in-depth verifications are required.

Information technology security (*sécurité des technologies de l'information*) - safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

Integrity (*intégrité*) - the accuracy and completeness of assets, and the authenticity of transactions.

National interest (*intérêt national*) - concerns the defence and maintenance of the social, political and economic stability of Canada.

Need-to-know (*besoin de connaître*) - the need for someone to access and know information in order to perform his or her duties.

Physical security (*sécurité matérielle*) - the use of physical safeguards to prevent and delay unauthorized access to assets, detect attempted and actual unauthorized access and activate appropriate response.

Protected assets *(biens protégés)* - assets whose unauthorized disclosure would reasonably be expected to cause injury to a non-national interest.

Protected information *(renseignements protégés)* - information related to other than the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to a non-national interest.

Reliability status *(cote de fiabilité)* - indicates successful completion of a reliability check; allows regular access to government assets and with a need to know to protected information.

Restricted access area *(aire à accès restreint)* - work area where access is limited to authorized individuals.

Risk *(risque**)*** - the chance of a vulnerability being exploited.

Security clearance (*cote de sécurité*) - indicates successful completion of a security assessment; with a need to know, allows access to classified information. There are three security clearance levels: Confidential, Secret and Top Secret.

Security incident *(incident de sécurité)* **-** compromise of an asset, or any act or omission that could result in a compromise; threat or act of violence toward employees.

Site access clearance *(cote spéciale d'accès*) - required for access to installations critical to the national interest or to restricted areas for special events.

Threat (*menace*) - any potential event or act, deliberate or accidental, that could cause injury to employees or assets.

Value (*valeur*) - estimated worth, monetary, cultural or other.

Vulnerability *(vulnérabilité)* - an inadequacy related to security that could permit a threat to cause injury.