REVIEW
DIRECTORATE

DIRECTION GÉNÉRALE
DE L'EXAMEN

REVIEW OF THE MANAGEMENT OF INFORMATION TECHNOLOGY

APRIL 2000

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

BACKGROUND

The presence of technology in the conduct of DFO's business is clear. The survey of departmental staff conducted as a part of this review in the summer of 1998 noted that 97% of staff have access to or use a computer in their day to day work.

Departmental Staff	%
Who have access to a computer in regular work activities	97
For whom information technology is necessary to deliver departmental responsibilities	81
For whom information technology is supportive of delivery of departmental responsibilities	69
For whom information technology is supportive of work with other departmental staff	72
Who use large scale custom designed applications	30
Who feel that their current system fully meets their needs	88
Who feel that their current system is sufficient for the next 12 months	74
Who have used the DFO Intranet in the past month	72
Who have used the Internet in the past month	82
Who use the Help Desk and find it good, very good or excellent	85
Who never call the Help Desk	24

The most valuable overall finding of this review is that DFO needs to manage information technology using clear business planning models that link current circumstances to future goals, include strong input from users, and clearly assess costs and technical implications.

Information Technology (IT) within DFO comprises all of the computer systems of the department, both hardware and software, and the networks linking them. Assets include over 8,000 personal computers as well as 18 large scale and custom software systems. These large systems do everything from providing a national recording system for fisheries violations to tracking the course of vessels at sea. A total of 94 computers are specially tasked as 'routers' to operate the WAN/LAN network. The technology enables employees of the department to carry out a host of functions including word processing, technical analyses, storing and transmitting data, doing research on the Internet, etc.

The focus of this review was to determine how well information technology was managed within DFO. The review, which was national in scope, addressed the following issues: the levels of capital and operating dollars spent on information technology; the management processes governing the planning and acquisition of information technology assets; the quality of service being provided; an analysis of recent patterns of IT utilization; security; and the use of the Internet.

It is important to note a number of key developments in managing information technology have taken place within the Department during this decade. In 1995, Corporate Services Information

Management and Technology Services Directorate (IM/TS) began the task of developing a standard Informatics Architecture for DFO. They invited IM/TS staff and clients from all regions and NCR to participate. The architecture initiative has improved the technical efficiency of the networks and ensured that they can operate as an integrated whole. The architecture initiative included a comprehensive harmonization of hardware and software

SUMMARY OF FINDINGS

Spending on IT in DFO represents a significant component of overall expenditures. DFO's spending on IT in 1997-98 was $66.9 million dollars which is 6.1% of total departmental spending. Expenditures were allocated into six categories

Category	**Expenditure (millions)**	**Per Cent of Total IT Expenditure**
Hardware	$22.7	34%
Consulting Services	$19.6	29%
IM/TS Salaries (excluding library and central records)	$12.7	19%
Telecommunications (non voice)	$8.9	13%
Software	$2.9	4%
Supplies	$0.1	1%

This represents an annual expenditure per full time employee (FTE) of $6,658. This figure does not include the salary figures for staff in programs who spend all or a significant part of their time managing IT.

We also compared IT expenditures in DFO for 1997-98 with those in other government departments with like mandates. DFO spends more than either Health Canada ($5,400) or Agriculture Canada ($6,000) but less than Natural Resources Canada ($9,500) or Environment Canada ($9,700). In response to a request from Senior Management (made during the Departmental Review Committee's discussion of the interim report), we also made some more global comparisons with expenditures in North American business as well as U. S. governments at the federal, state and local level. These data showed large variations and that IT expenditures rise dramatically (16 fold) between organizations with a moderate commitment to IT solutions and those with more aggressive implementation.

DFO's overall IT expenditure of $6,658 per FTE breaks down to $2,818 (42%) by IM/TS and $3,840 (58%) within programs. In IM/TS, the largest expenditure is on salaries, followed by hardware, consultants, and data communications. High salary expenditures reflect the substantial body of in-house specialized expertise in IM/TS. In programs, where many of the large scale and custom software programs are developed, the largest expenditure is on consultants (42%). Given this large consultant expenditure, one could ask why IT managers in programs are not making greater use of the in-house expertise residing within IM/TS. This is an area where significant cost savings could be realized. The reason it presently is not happening is due to the highly decentralized and uncoordinated decision-making process now in place for

managing IT. Problems that are found in several sectors or regions have sometimes had specific, different and duplicative solutions developed. Roles, responsibilities and accountabilities need to be better defined. The following example illustrates this concern.

The department's current provider of telecom services has indicated that similar services are being purchased separately by the Coast Guard, and by IM/TS. They further indicated that savings could be achieved if all circuits and services were purchased in an integrated way. The review recommends that the Coast Guard, in cooperation with Corporate Services IM/TS and Public Works and Government Services Canada, Government Telecommunications and Informatics Services (GTIS), assess the degree to which cost savings can be achieved through harmonizing acquisition of these networking services. On a more general note, such duplication could be avoided if there were a clearer decision-making process to ensure that all IT investments are fully assessed, both for their support of program needs and for their compliance with departmental standards and architecture. We recommend that Senior Management define and clarify roles, responsibilities and accountabilities for the management of IT.

The last three years have seen several "one-off" investments in IT. Each of these has provided measurable benefits in line with the objectives of the investment. What has not been addressed is the provision of long term, stable funds, on an ongoing basis, to keep core activities operating and evolving in response to needs. Such a core functionality would likely include the WAN/LAN, operating systems, the desktop suite, help desk, and IT portfolio managers. It would be administered by IM/TS, both in Corporate Services and in the Regions.

Of all of the components in this core functionality, the network (including e-mail, the office desktop and user help) is the most important, mission critical component. Electronic mail, file sharing and integrated financial and personnel systems can occur only when the network is functioning properly. The review did a detailed topology of how the network operates and uncovered significant unevenness in its administration. A WAN is administered from the NCR, and several LANs are administered regionally as well as in the NCR. Each of these components is operated and administered in different ways in each region. Core funding has the advantage of eliminating this unevenness in administration and the level of service being provided to users. Also, we learned that significant cost savings could be realized if a consolidated, Department wide architecture for the WAN were created. Core funding would also eliminate the presently unevenly administered system of chargebacks for LAN management services in the NCR and some regions.

In order for the concept of a core functionality to work, there must be a clear definition of what is and is not included as well as an explicit and verifiable assessment of what level of funding should be provided. The review recommends that core funding be provided for the network, desktop, help desk and portfolio management components.

Clarifying accountabilities and core funding are necessary to strengthen the management of information technology. Such strengthening can only take place when the people responsible for IT management in IM/TS and programs make a greater effort to consult, learn and co-operate with each other. This includes a more concerted effort in consulting with and listening to users of information technology.

The concept of the 'portfolio manager' now used at NCR and in several regions is one approach that appears to work well in furthering consultation and cooperation. In this approach, IM/TS assigns an individual to become expert and provide continuity in meeting the IT needs of a specific program area. Where these positions exist and links to the program areas are nurtured, this is clearly a 'best practice'.

The status of consultation mechanisms between IT providers and users was examined as well. There currently are client/provider consultative mechanisms in various regions and sectors but no definable pattern exists. In the regions, we found some committees that had been struck for specific projects. Others were organized on a multi-sector basis or between one sector and IM/TS to address specific program needs. These were most apparent in Pacific where IT resources can easily be identified as resident in programs. At the national level, there was no client/provider committee structure at the time this review was conducted. In early 1999, a national Informatics Steering Committee (ISC) was formed. This committee is expected to become a key forum for taking action on many initiatives recommended in this review.

One example pointing out the need for a much more coordinated program of consultation is the rollout of Microsoft Office 97' desktop package now partially replacing Office 4.3. The review examined the management processes undertaken to justify the decision to upgrade the software and the degree to which users were consulted. The new version of the package was purchased as DFO's national standard even though a business case had not been developed showing the incremental benefits and despite inventory information which showed that a substantial number of users would be unable to move to the new standard. In addition, clients were not consulted on the need for the increased capability that Office 97' might bring. The cost of the Office 97 licence was estimated at about $700,000. However, the review determined that the introduction generated a training need that cost an estimated additional $900,000. The review recommends that future system- wide upgrades must be based on a full business case incorporating user input and must incorporate the cost of hardware upgrades and training. In addition, the review also recommends that Corporate Services IM/TS take the lead in developing a mechanism to address training needs that have been created by recent introductions of new software.

The review examined the degree to which the management of IT is presently conforming to standards and administrative policies. Such standards and policies most often pertain to questions of "who does what?" and "how are things done?". The existing lack of such policies and standards and the present degree of compliance or non-compliance with those standards, when they do exist, are illustrated by the following examples.

At present, DFO has a contract with the Government Telecommunication and Informatics Directorate (GTIS) of Public Works for the management of the IM/TS WAN. GTIS, in turn, has contracted out the management of the system to a local firm, NUVO Networks. The review examined the detailed Services Level Agreement (SLA) which DFO has negotiated with GTIS. The review team found a lack of compliance in meeting the performance standards stipulated in the contract in the area of reporting and managing "bandwidth" (the level of traffic in the system). Also, GTIS, who is responsible for making architecture recommendations for the WAN, has not done so. Given the failure to perform to standards, the review recommends that

Corporate Services IM/TS develop a comprehensive needs statement for the performance of the WAN. Remedial action should be taken if service levels are not met.

Another important area where the review team found there to be a serious failure in providing consistent service standards pertains to the management of the Internet. The departmental interface with the Internet is managed with six Internet "firewalls " throughout the NCR and regions. These are presently being managed inconsistently, without the benefit of a standard. The nature of the WAN/LAN is such that the least permissive firewall sets the risk for the entire system. The architecture of the electronic mail system was also identified as one with a high exposure to risk from the Internet. Given the present apparent vulnerability of the system, the review recommends that Corporate IM/TS conduct a threat and risk assessment on internet access and the configuration of the e mail systems to assess present levels of risk.

The review uncovered numerous other areas of inconsistency that could benefit from standards and consistent policies. The review recommends that Corporate Services IM/TS in Regions and NCR work with clients to establish reasonable and effective means for standardizing the following: firewall rules, levels of service, services that qualify for 24 hour support, services that must have no single point of failure, and service to remote locations, including ships.

A study of existing, large-scale systems was undertaken in the NCR and Maritime Regions to ascertain how they had been managed from conception to implementation. Large-scale systems were defined as costing over $500,000, delivered to more than 100 employees or implemented across multiple locations. At least two of the systems looked at in this review, the Departmental Violations Information System and the Habitat Referral Tracking System (HRTS), grew from an anticipated cost of less than $100,000 to an as delivered cost of over $1 million. The original estimate for HRTS did not reflect development, implementation or training costs, or the substantial costs associated with changing it from a WordPerfect based system to one based on Microsoft Word. Changes in the network operating system and the implementation of firewalls also caused the price of HRTS to increase to a final cost ten times greater than the initial estimate. Where detailed plans were absent costs were higher than anticipated and in some cases, deliverables did not appear in the year they were expected. Overall, it was found that systems that were developed through project specific teams that included staff from Corporate Services and Regional IM/TS as well as program experts and consultants tended to work best. Maritimes and Laurentian Regions have developed an effective planning system for large-scale systems. The review recommends that DFO ensure that all large-scale IT systems are assessed using a comprehensive project assessment and planning tool.

As part of its mandate, the review also addressed issues pertaining to present IT utilization and how this affects issues like the security of information, what constitutes "acceptable use " for DFO employees using the Internet and DFO communications.

The user survey revealed that of all of the shared IT services, it is electronic mail that is the most valued. The Coast Guard recently commissioned an extensive security study, which determined that the current e-mail system could be intercepted and tampered with. The review found no policy informing users of the security level of information that can be sent via e-mail. Therefore

it is recommended that Corporate Services IM/TS notify users of the security level of DFO's current system and the types of information that can and cannot be transmitted

At present, all DFO users have access to the Internet. The average number of internet responses or "hits"per day (per full time employee) has been averaging about 28 at NCR, Maritimes, Newfoundland and Central and Arctic Regions. It has been averaging about 42 in Laurentian and 67 hits per day in Pacific Region. It was determined that about 10% of present DFO internet traffic is accessing subject matters with no apparent business purpose (including ads, news, business, sports and sex etc.). DFO has not monitored which Internet sites are being accessed. The review recommends that DFO provide an 'Acceptable Use Policy' to provide clarity on what is, and what is not acceptable for DFO employees using IT resources. An acceptable Use Policy was issued on May 28, 1999, while this report was being reviewed by DFO staff, prior to its release.

Finally, the review also briefly examined how IT has facilitated communications both within as well as with those outside of DFO. With respect to internal communication, the user survey provided some evidence of information 'overload'. There is no policy to indicate what types of information are appropriate for electronic distribution. The lack of clear policy direction is similar with respect to publishing on the Internet. The review identified that DFO spends about $2 million annually on Internet publishing. No mechanism exists to ensure that what is published is valuable and contributes to departmental objectives. Communications Directorate has the responsibility of enforcing departmental and Treasury Board standards but indicated they have not done any monitoring. The review recommends that Corporate Services IM/TS work together with Communications Directorate to ensure that an orderly and reasonable approach to the use of electronic communications is identified**.**

2.0 INTRODUCTION

2.1 BACKGROUND

Information technology is now an essential tool for staff in DFO in the delivery of departmental programs. This technology includes not only large and small computers but also electronic interconnection systems that link IT devices together. Computers themselves have evolved from research tools on room-sized mainframe computers and "typewriters with memory" into an interlinked infrastructure as indispensable as our buildings and telephones. According to the June 1998 telephone survey of the department conducted by PriceWaterhouseCoopers for this review, 97.8% of respondents reported that they use a computer in their *regular* work activities. Furthermore, 94% report that computers are essential to deliver their departmental responsibilities.

Originally, computers were simply stand-alone tools, used by specific individuals, programs and groups. As their use became more widespread, small groups became organized and tethered together in networks. At first, this was local "work groups", then larger and larger assemblages and now our current national system with continuous links to all but the most remote offices and ships (which are served through dial-up access, as well as cellular and satellite links).

Initially, the growth of DFO's architecture was within the department's work groups. Some, like Small Craft Harbours and Fish Inspection (which has since left the department), went so far as to establish a national stand-alone network; others implemented within-building links by "sector"; still others, particularly Science, began to work with colleagues inside and outside DFO using the Internet. The Coast Guard maintained inter-city electronic links directly and through Transport Canada to connect key offices across Canada long before merging with DFO. While steps have been taken to ensure that electronic mail and desktop applications in Coast Guard operate across the wide area network (WAN) managed by IM/TS, certain technical elements of the two systems remain very similar and are administered separately.

Following a suite of studies by Price Waterhouse of the department's Information Management/Technology Services (IM/TS) Directorate done between 1992 and 1994, as well as extensive work by IM/TS within DFO, a standard "architecture" emerged. Through the provision of targeted one-time funding, a more integrated uniform system was implemented. The DFO Informatics Architecture document and the subsequent infrastructure initiatives have dramatically improved the technical interoperability of the network and its systems. This process was effective in ensuring that the networks managed by IM/TS and Coast Guard could operate as an integrated whole. Issues remain, however, regarding planning, funding and managing the assets across the department so that they function effectively to support the department's needs in a cost-effective way.

While we are now physically linked together, the management of IT still differs widely across the department, even within one region or sector. Intersectoral tensions exist and problems that are found in several sectors or regions have sometimes had specific, different and duplicative solutions developed without reference to the benefits that a higher level of coordination would have brought.

The management of IT is important as, over the past three fiscal years, DFO spent approximately $66.9 million per year (6.1% of overall spending) on IT (based on an analysis of spending by line object). This breaks down to about $6,658 per employee per year. While directly comparable data from other federal departments with a similar mission are not available, a comparison of non-salary expenditures has been conducted. Using these data, DFO's expenditures are in line with those of other similar Canadian federal departments (i.e. lower than Natural Resources and Environment while higher than Agriculture and Agri-Food, and Health). A table of these expenditures can be found in section 3.2.2 of this report.

2.2 OBJECTIVES AND SCOPE

The management of IT was assessed from the following perspectives:

- a general assessment of operating and capital dollars and FTE's directly involved in the management of IT
- the implementation of an appropriate interface for policy and planning among all managers of IT across the department, and between these managers and their respective clients
- the nature and effectiveness of the strategic planning tools in use in all parts of DFO that govern the acquisition and management of IT
- the department's ability to support and promote the use of technology to sustain and improve:
    1. program delivery to clients
    2. staff productivity
    3. communications within the department
    4. provision of information on program results and financial status to managers
- compliance with Treasury Board policy

A sample of recent investments was assessed to determine if they were evaluated and implemented within an information management framework. The examples for review were drawn from large scale systems found in all relevant sectors. Recent investments in hardware, software, and services include: Abacus, Peoplesoft, Windows NT server, Office 97 upgrade, Microsoft Exchange/Outlook, the Habitat Referrals Tracking System, the Departmental Violations system and the implementation of a new desktop hardware standard. A summary analysis of the strategies and consultation that preceded these acquisitions was made. It was important to identify where projections regarding cost savings and other benefits such as decreased downtime and increased reliability were made prior to implementation of these system changes, as well as the attainment of the anticipated benefits.

The scope of this review included the management of hardware, custom and commercial software, interlinking and network communicating tools, fixed installations and portable hardware. Also included was IT that is provided to the department on a lease, rental or license basis (excluding local and long distance voice telephone). As a key part of this review the delivery and support mechanisms were identified and assessed.

This review coordinated its work with the Review of Corporate Services Redesign and the Governance Options Project, and took into account all relevant inventory work that has already been completed. As well, information from recent studies that bear on the management of IT (e.g. Peoplesoft, Abacus) was utilized where appropriate.

2.3 METHODOLOGY

The review was conducted from February to December 1998. Specific studies were conducted, some by staff in DFO's Review Directorate and some by consultants under their direction. Significant efforts were made to work closely with key departmental personnel as the review moved forward.

There were three major and five minor lines of enquiry. Only one of these, the user survey, will be released as a separate report. In addition to these lines of enquiry, every major DFO study of IT, networks, the informatics function and IT security conducted since 1991 was assessed for its currency and relevance to the objectives of the study.

The three major components were the user survey, the analysis and benchmarking of department-wide expenditures on IT and a review of the WAN, Internet and security.

1) The user survey of departmental staff was conducted by telephone in the summer of 1998. It presents results by region and by sector with 90% accuracy. The survey results were compared to similar surveys conducted in other organizations. Areas of key achievement (best practices) and areas requiring attention were identified.

2) Departmental expenditures covering the three most recent fiscal years (1995-96, 1996-97 and 1997-98) were analyzed and benchmarked. IT-related objects of expenditure were identified and mapped across the systems in old DFO and in the Coast Guard through the three-year period. All expenditures in the department were sorted by region and by sector, with old DFO being reported by business line and the Coast Guard being reported by responsibility centre. The expenditures were graphed and trended, with inter-region and inter-sector comparisons being made. The figures were then benchmarked against Full- Time Equivalents (FTEs) (as found in the Salary Management System) and against total expenditures (by region, by sector and nationally). The most important analysis was to look at inter-region, inter-sector and inter-year comparisons. Department-wide expenditures were then compared against expenditures made by the three other "natural resource" departments and Health Canada. Broader benchmarking against North American business and U.S. federal, state and local governments was also done. Although these are somewhat remote from DFO's situation, they help to determine if the department is in line in a larger context and were requested by senior management during an interim reporting meeting.

3) The third major study was conducted on the "backbone" components of the network. This included the WAN connecting all major departmental centres, its capacity and the utilization of that capacity as measured by daily reports commissioned by the department. The study also looked at patterns in Internet traffic at each of the department's six

"firewalls" (devices that interface between DFO's network and the Internet). The purpose of this component was to assess the volume and nature of Internet use and the degree to which this is a cost factor for the department's infrastructure. The final component of the study was an assessment of security issues. This component focused on the implementation of reasonable and necessary security measures regarding protected information, physical security of Local Area Network (LAN) and WAN devices, and security against unauthorized access from any source (including the Internet).

The five minor components were:

1) an analysis of departmental IT management policies, committee structures, and planning documents to assess their scope and efficacy, as well as the degree to which they relate to DFO program needs and incorporate client input;

2) an analysis of the management of departmental large-scale custom software systems which operate at either a national or at a regional level to assess the business case that was made, as well as the procurement and development processes used and the degree to which the product met the initial objectives and cost estimates;

3) an analysis of current management practices and policies surrounding remote access to DFO computer systems to assess compliance with policies, costs and the degree to which DFO has implemented teleworking opportunities;

4) an analysis of the management processes used to decide on a recent change to the standard departmental office suite (from Microsoft Office 4.3 to Microsoft Office 97) that affected every user in the department. This was done in order to identify what implicit and explicit management processes were used to identify the business requirement, and the specific product, as well as the degree to which the users were a part of the decision making process, and what business related improvements have been delivered to departmental users as a result of this change; and

5) an analysis of the management of Web publishing on both the Internet and the internal government-wide Intranet to determine the degree to which this new communications channel has been subject to the same standards, constraints and considerations as printed publications, as well as to assess the costs and, where possible, the effectiveness.

3.0 OBSERVATIONS

3.1 INFORMATION TECHNOLOGY IS ESSENTIAL

Given the long history that DFO scientists have had using computers, as well as early use of proprietary systems for such office functions as Ministerial correspondence, reviews and assessments of the department's use of IT are as old as the technology itself. Only the most recent IT related studies since 1991 were looked at as a part of this review. In virtually all of these recent studies there has been a consistent call for a higher level of organization and integration in the use of computers and the achievement of a greater level of support for the department's programs from what is now generally called IT.

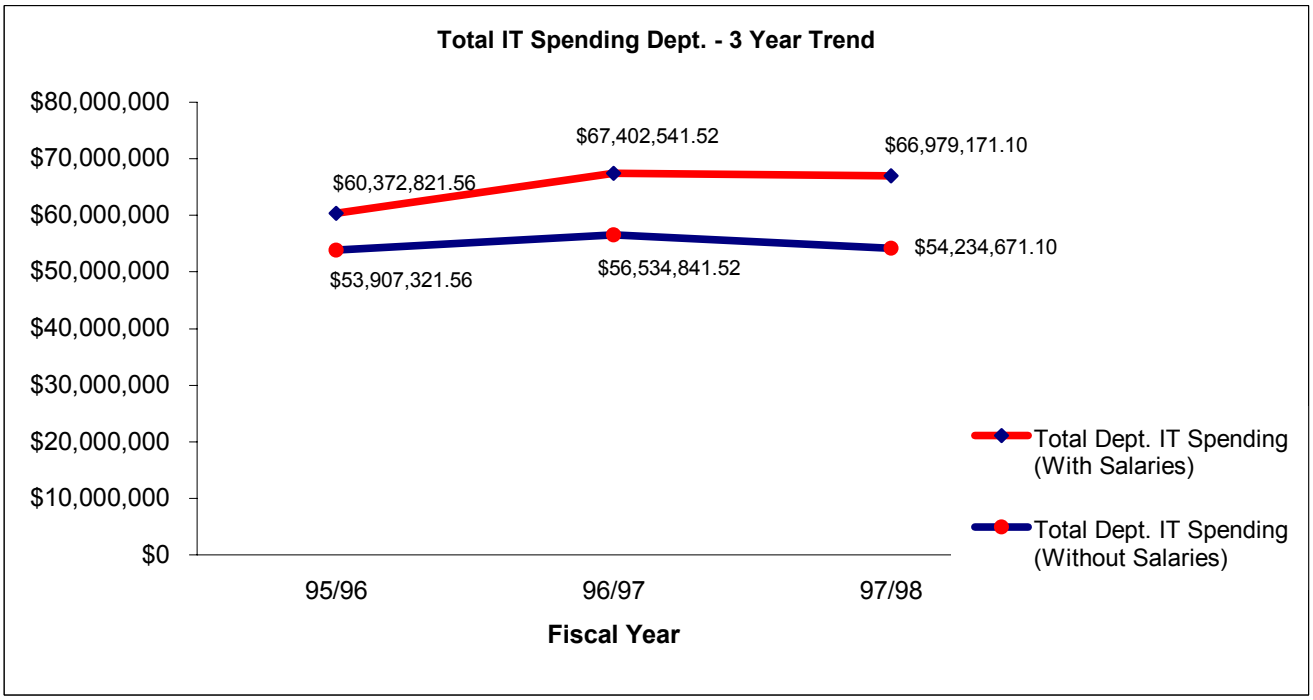
While departmental spending on IT occurs in every region and sector, 56% of the 1997-98 IT spending was in Corporate Services (42% of the department's spending was in the IM/TS component of Corporate Services.) The sector with the next highest level of spending was Coast Guard which spent 25% of the departmental total. This review looked at spending in all sectors and regions, but more closely at IM/TS spending. This reflects not only the highest area of spending but also the group with the core responsibilities for managing IT related matters in DFO. The other areas in Corporate Services with high IT spending, Abacus and Peoplesoft, have already been subject to detailed review and have not received detailed assessment in this review.

The networking of computers (that can share files and e-mail that are compatible) is the most important "value added" to the department as a whole. While individual machines operating specialized systems can be mission-critical for specific program components or even entire programs, the communications advantages of the network working as a whole make the network possibly the most mission-critical IT asset in the department. The network, in the various studies that underpin this report, is clearly essential to program delivery. Electronic mail (e-mail), file sharing and integrated financial and personnel systems can occur only when the network is functioning properly. It is as essential and as basic as the buildings in which we work and the vehicles that we use to deliver our programs.

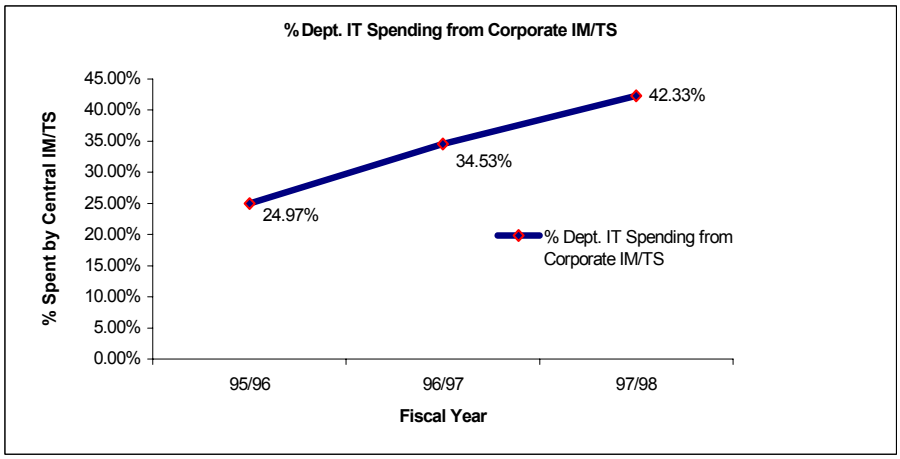
The review found significant unevenness in the administration of the network, service levels and chargebacks, user support, the involvement of clients and the implementation of the standard office suite. The standard office suite and e-mail comprise the two national software standards that support communication among all parts of DFO. E-mail is well integrated and generally functions in an orderly and reliable way. A WAN is administered from the National Capital Region (NCR) and several LANs are administered regionally (as well as in the NCR). Each of these components is operated and administered in different ways in each region. In some regions, there is core funding for IM/TS and, in others, there are chargebacks which vary widely in the amount and scope of services which are linked to the chargeback.

3.2 EXPENDITURES BY DFO ON INFORMATION TECHNOLOGY

3.2.1 Information Technology Expenditures



An analysis of all departmental expenditures on IT was conducted for 1995-96, 1996-97 and 1997-98. Although these years include the first year of the DFO-Coast Guard merger and several cases of one-time funding in various areas, the expenditure patterns are quite stable.



Over the three years, while the departmental total has remained fairly stable, the amount that is expended through IM/TS has grown from 25% to 42%. This reflects in part special

"infrastructure" spending in 1997-98 and also the expansion of "service level agreements" which transfer funds from programs to IM/TS.

The department's IT expenditures on a per FTE basis are shown below.

Exhibit 3.2.1.1 Departmental IT Expenditures Per FTE (1997-98)

Component	Expenditures
All of DFO	$6,658
Spent Outside IM/TS	$3,840
Spent by IM/TS	$2,818

Exhibit 3.2.1.2 1997-98 IM/TS Chargebacks Per Region

Region	Chargeback Per FTE
Newfoundland	$0
Maritimes	$1,050
Laurentian	$0
NCR	$1,000
Central and Arctic	$0
Pacific	$0

The two tables above, when taken together, confirm that the chargeback system for IT services is uneven and that the amount charged back bears no evident relationship to actual expenditures by the IM/TS groups in individual regions or the NCR.

Exhibit 3.2.1.3 Analysis of 1997-98 IT Expenditures Per Departmental FTE

Expenditure Type	IM/TS Expenditures Including Salary	IM/TS Expenditures (non Salary)	Program Expenditures (non Salary)
Expenditures per FTE	$2,818	$1551	$3,840
Salaries	45%[1]	0%	0%[2]
Hardware	28%	51%	38%
Consulting Services	12%	22%	42%
Data Communications	11%	20%	15%
Software	4%	7%	5%
Supplies	<1%	<1%	<1%

[1] Throughout the report IM/TS expenditures on Libraries and Central Records have been removed where information about expenditures provides for such a determination. Data are from DFO's Financial Management Reporting System, Abacus and the Salary Management System.

[2] This study did not attribute program salary dollars to IT activities. The analysis instead is of expenditures by line object, which is the most readily verifiable information. A larger A-Base type review would be required in order to accurately determine salary expenditures directly attributable to the management of IT.

This table, based on line object groupings, demonstrates that the amount spent within programs ($3,840) is similar to the amount spent by IM/TS ($2,818), although the products and services are very different. Even though IM/TS retains consultants for such functions as Help Desk, their largest expenditure is on salaries, followed by hardware, consultants and data communications respectively. This contrasts sharply with the profile in programs. Here, where many of the large scale and custom software is implemented, 42% of the spending is on consulting services. The IM/TS salary figure confirms that there is significant expertise within the department. It is possible that more effective use of this experience could reduce the need for programs to spend on consulting services. It is also important to note that the expenditures on data communications are of a similar magnitude in programs (15%) and IM/TS (20%). While some data communications are charged back, this suggests that programs are operating data communications systems entirely within program areas. Given the funding pressures within DFO at this time, there would appear to be an opportunity for savings if some of these data communications systems were consolidated. Anecdotal discussions with the Government Telecommunications and Informatics Services component of Public Works and Government Services Canada (GTIS), which supplies WAN services to Corporate Services and digital circuits to the Coast Guard, indicate that even harmonizing the acquisition of services would lead to savings, and that further integrating the management of these two systems could lead to even greater savings. While the Coast Guard inter-city links, which are used for navigation-related information (including digitized voice communications), needs a high level of reliability, as GTIS is the supplier to both, it would seem that harmonization of the management of these similar systems within DFO should be assessed.

Exhibit 3.2.1.4 Analysis of 1997-98 IT Expenditures Per FTE By Programs and IM/TS By Region

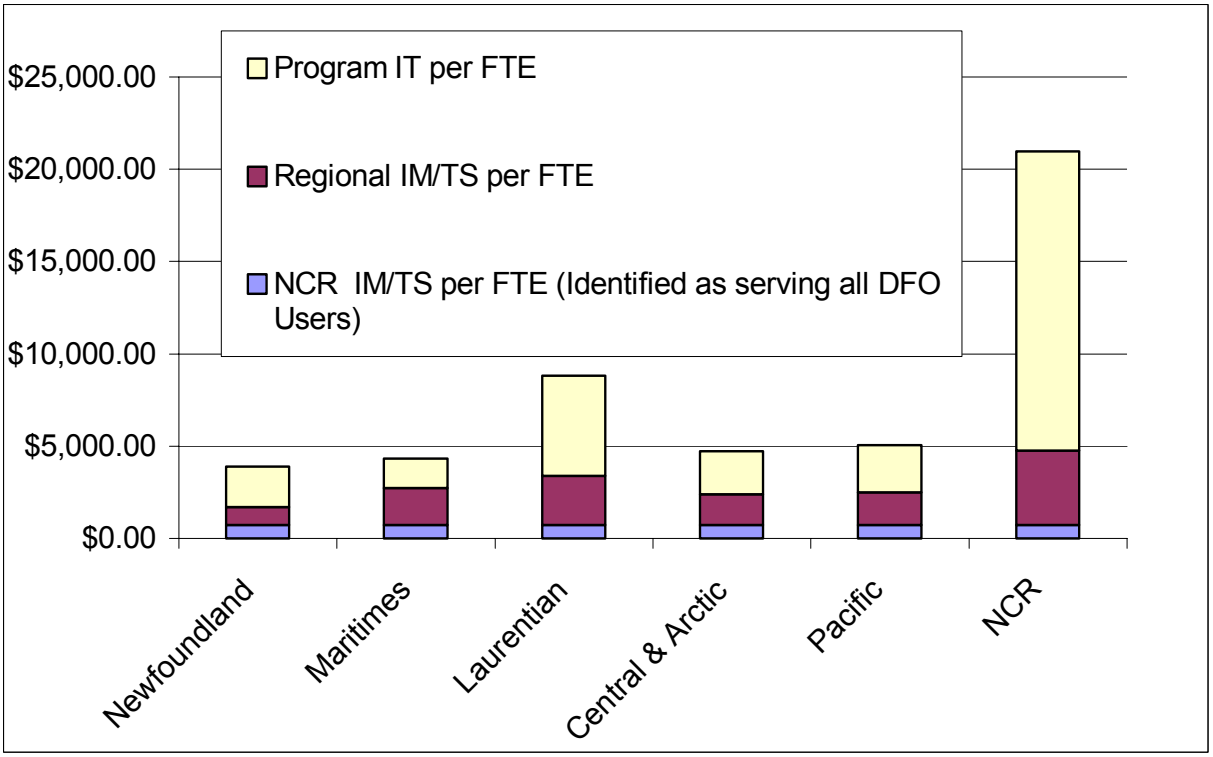


Exhibit 3.2.1.5 1997-98 IT Spending Per FTE Per Region

Region	NCR IM/TS Spending Identified as Serving All DFO Users	Expenditures By Regional IM/TS	Expenditures By Programs on IT	Regional IM/TS Spending as Percentage of Program Spending on IT in that Region
Newfoundland	$748	$938	$2,200	43%
Maritimes	$748	$1,976	$1,611	123%[3]
Laurentian	$748	$2,649[4]	$5,419[5]	49%
Central and Arctic	$748	$1,638	$2,352	70%
Pacific	$748	$1,740	$2,558	68%
NCR[6]	$748	$4,017	$16,210	25%
Average Cost Per FTE Across DFO in 1997-98: $6,658				

The foregoing table shows that delivery models vary widely from region to region. Even the direct expenditures (including salaries) of IM/TS in each region vary from 25% of IT expenditures by programs in the NCR to 123% of the expenditures by programs in Maritimes. The situation in Maritimes reflects the significant transfer of program monies into IM/TS for expenditures under service level agreements. While IT expenditures in the NCR are the highest (four times that of Newfoundland), the NCR is also where many national program systems are developed and operated. These systems (e.g., the Departmental Violations System, the Habitat Referrals Tracking System and others) bring workload that is unique to the NCR, with the exception of the Coast Guard INNAV system which is being developed in the Laurentian Region for application in the East Coast. When IM/TS costs are shown as a percentage of these national systems, the NCR (even with the highest overall expenditures per FTE) comprises the smallest component.

Providing an adequate level of funding to the network and related elements in all regions as well as to the WAN (which is administered in the NCR for the entire department) is appropriate given the essential nature of the networking function. One way of providing the necessary funds could be that funds would be provided directly from the department's base at an early stage in the budgeting process. It is important to note that the portion of the department's IT expenditures attributed to the WAN managed by IM/TS is very small (just over 10% of all IT spending in DFO) when compared to other costs, notwithstanding the critical support this WAN provides to departmental activities.

[3] Under service level agreements, over $5 million is transferred from programs for expenditure by IM/TS.
[4] Laurentian Region has reported that they began large scale year 2000 related spending in 1997-98 which may contribute to this higher figure.
[5] This large expenditure includes two specific components. The Laurentian Region initiated large scale year 2000 projects in 1997-98. Further , the Coast Guard INNAV system, a multi-million dollar custom system for the Atlantic that is being developed in the Laurentian Region, is a significant and anomalous component that pushes up program spending per FTE.
[6] In this analysis, the NCR is treated like a region, NCR IM/TS reported an expenditure level that they identify as benefiting all users in DFO.

In those regions where IM/TS has instituted chargebacks, considerable effort is expended in identifying what is charged back for the network and related elements. A measurable effort is also spent in chasing "bad debts" where programs fail to provide the agreed-upon fees, especially where some services (like the WAN) cannot reasonably be removed to force payment. More consistent approaches (on a per FTE basis) would seem to be possible given the wide variation shown above.

Exhibit 3.2.1.6 1997-98 IT Expenditures Per Sectoral FTE By Sector

Sector (All Regions)	Per Sectoral FTE Expenditure
Corporate Services	$27,385[7]
Policy	$5,605[8]
Science (including Oceans)	$3,680
Coast Guard	$3,513
Fisheries Management	$2,903
Average Cost Per FTE Across All DFO in 1997-98: $6,658	

The above analysis shows that with the exception of Corporate Services, which houses not only the IM/TS function but also Abacus and Peoplesoft, the program expenditures per FTE on IT are on the same scale. This is especially noteworthy as Science is often considered as a "large-scale user" of IT; however, on a per FTE expenditure basis, it is in line with the Coast Guard and similar to Fisheries Management. It is important to note that, given the support role that Corporate Services has for the department, the "per Corporate Services FTE" figure cannot easily be compared with expenditures in other sectors, but has been included for completeness.

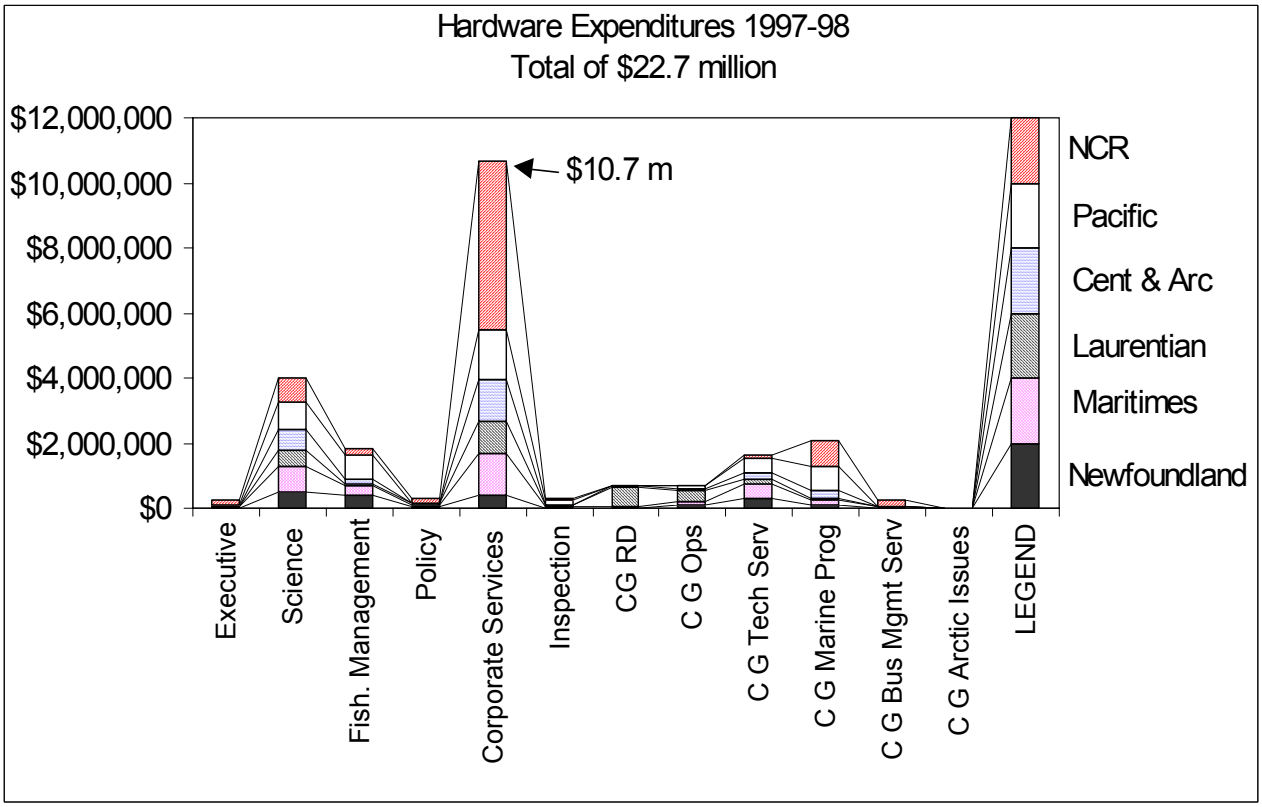
The last three years in DFO have seen several "one-off" investments in IT. Each of these has provided measurable benefits in line with the objectives of the investment. What has not been addressed is the provision of sufficient funds, on an ongoing basis, to keep these core activities operating and evolving in response to needs. These "one-off" investments (such as the Common E-mail and Infrastructure project) can solve specific "catch up" problems: however, these sorts of urgent catch up/rust out expenditures can be avoided through a recognition of the need for ongoing maintenance of the core functionality. This core functionality can be derived through the client/provider business line consultations recommended elsewhere in this report, but would likely include the WAN/LAN, operating systems, the desktop suite, help desk and IT portfolio managers, and the necessary needs based evolution of these systems.

The department's expenditures fall into four large line object groupings. A comparison of the spending patterns between DFO and other departments with similar missions follows. The spending patterns, when presented by line object groupings, by sector (and business line in Coast Guard) by Region help to identify how IT management strategies differ. The information is presented by line object grouping, as follows: hardware, software, consulting and data communications. The sectoral and business line categories represent individual bars, and the

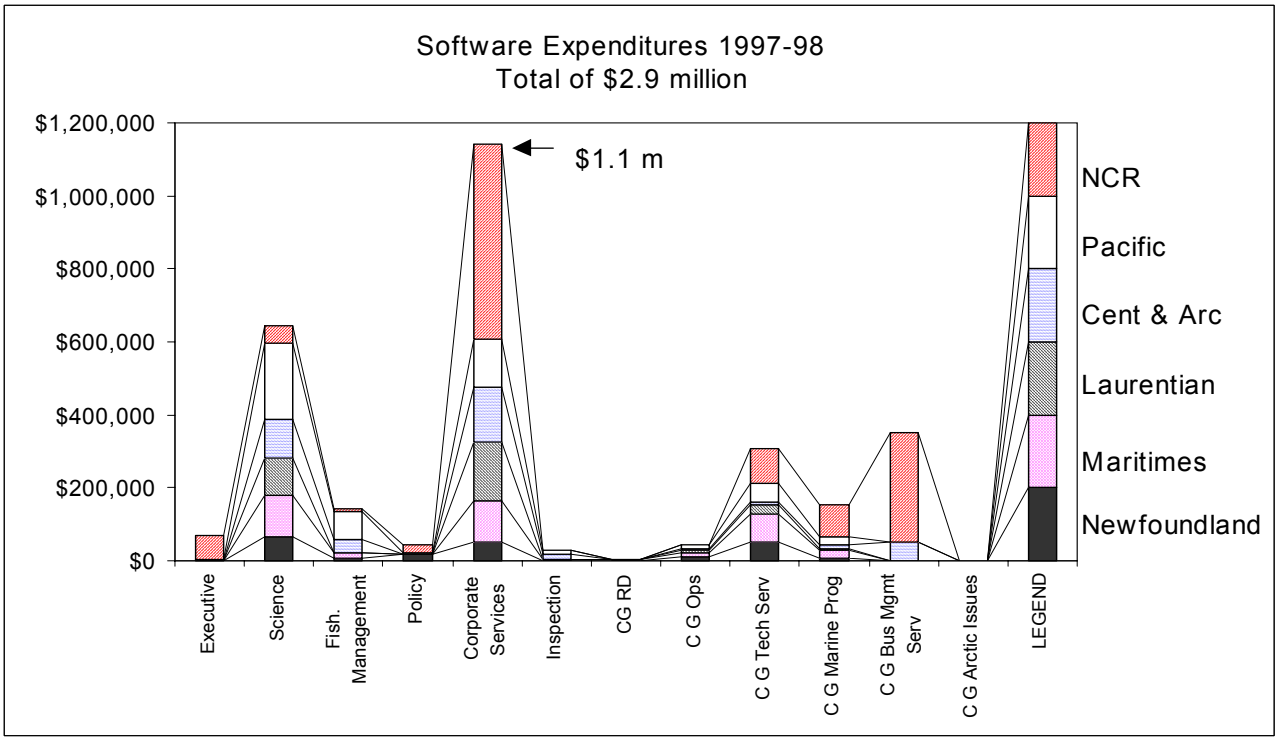
[7] This includes not only IM/TS support for the department but also Abacus and Peoplesoft and others, which are also support for all program areas.
[8] The two largest components of this are consultants in Maritimes ($320,000) and hardware in the NCR ($160,000)

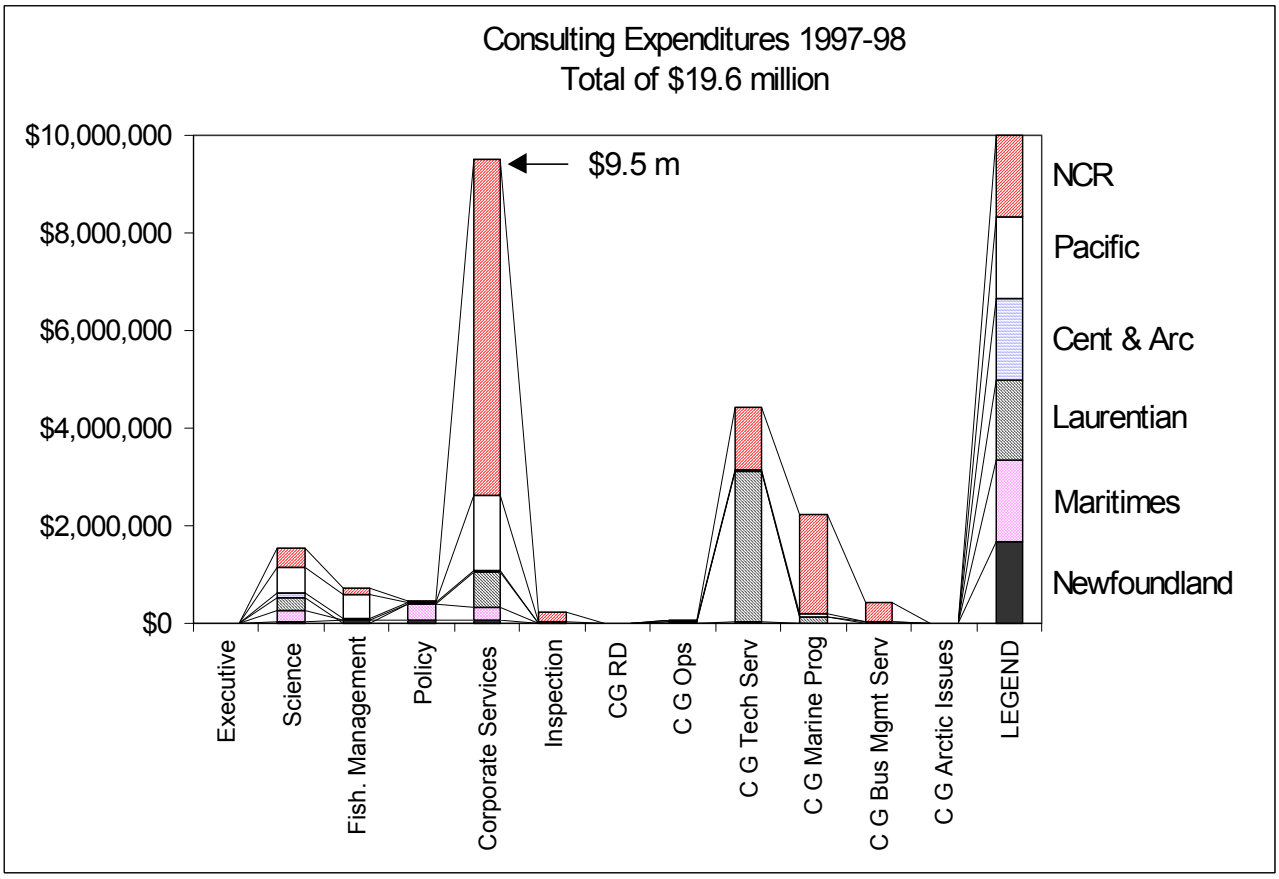
region where the spending took place is represented by a consistent marking scheme. As the graphs change in scale the value of the highest bar is identified on each graph

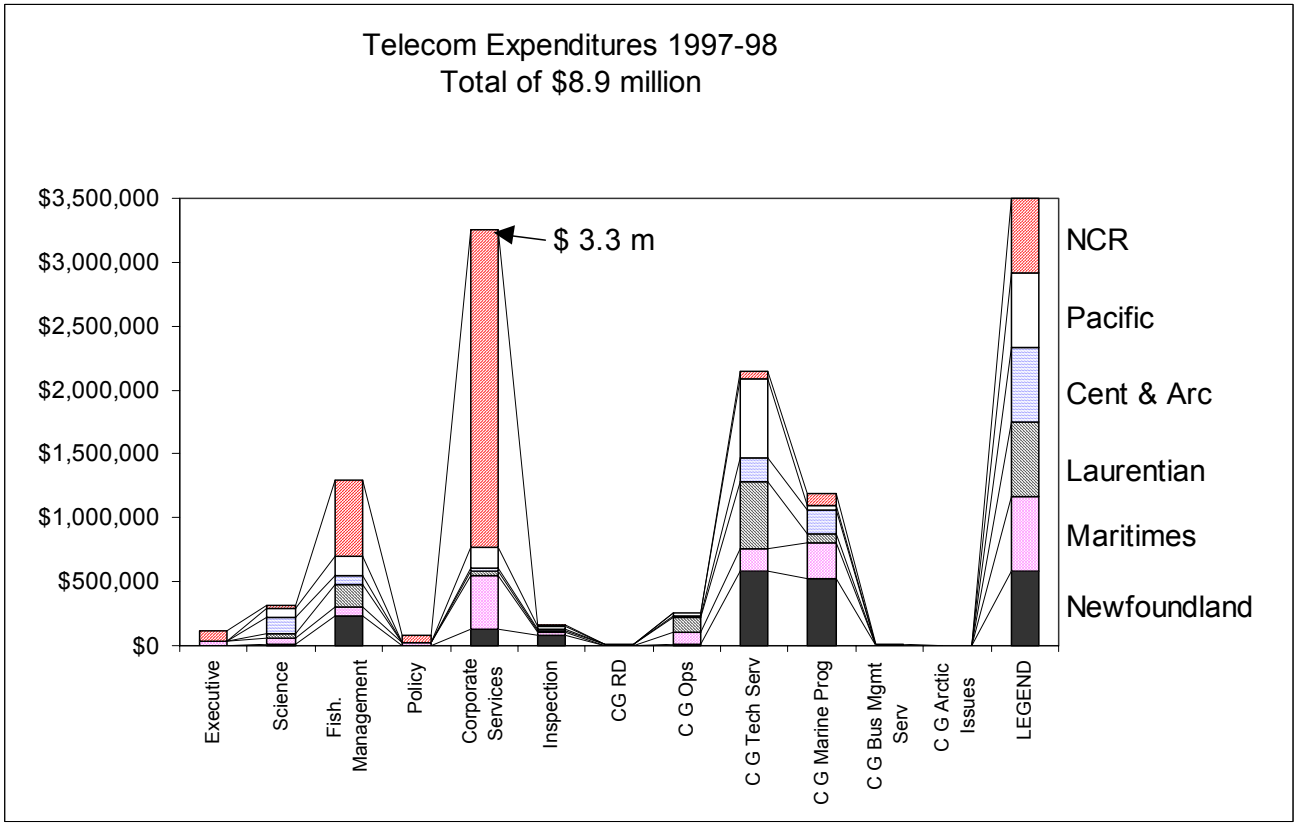
Exhibit 3.2.1.7 1997-98 IT Expenditures By Line Object Grouping By Region and Sector or Business Line[9]



[9] The Fish Inspection group appears in these graphs, as it does throughout the report as it was a component of the department during the three fiscal years analysed for this review. Its inclusion allows for the verification of results against consolidated departmental reports which include all sectors and regions.


Software Expenditures 1997-98
Total of $2.9 million
$1,200,000
$1,000,000
$800,000
$600,000
$400,000
$200,000
$0
$1.1 m
NCR
Pacific
Cent & Arc
Laurentian
Maritimes
Newfoundland
Executive
Science
Fish. Management
Policy
Corporate Services
Inspection
CG RD
C G Ops
C G Tech Serv
C G Marine Prog
C G Bus Mgmt Serv
C G Arctic Issues
LEGEND


Consulting Expenditures 1997-98
Total of $19.6 million
$10,000,000
$8,000,000
$6,000,000
$4,000,000
$2,000,000
$0
$9.5 m
NCR
Pacific
Cent & Arc
Laurentian
Maritimes
Newfoundland
Executive
Science
Fish. Management
Policy
Corporate Services
Inspection
CG RD
C G Ops
C G Tech Serv
C G Marine Prog
C G Bus Mgmt Serv
C G Arctic Issues
LEGEND



3.2.2 Expenditure Comparisons With Others

Expenditure data (by line objects) from all federal departments and agencies were analyzed. While each department is different, the expenditures of the three other "natural resource" departments (Environment, Natural Resources, and Agriculture and Agri-Food) and Health Canada were chosen as sufficiently similar to merit comparison.

All departmental expenditures were "benchmarked" as costs per FTE and as a percentage of the overall budget (less grants and contributions). As noted, DFO's costs in this example are derived from the same tables as the other departments and therefore do not include expenditures (such as IM/TS salaries) that are included in all other parts of the review.

Exhibit 3.2.2.1 1997-98 IT Expenditures in Related Departments

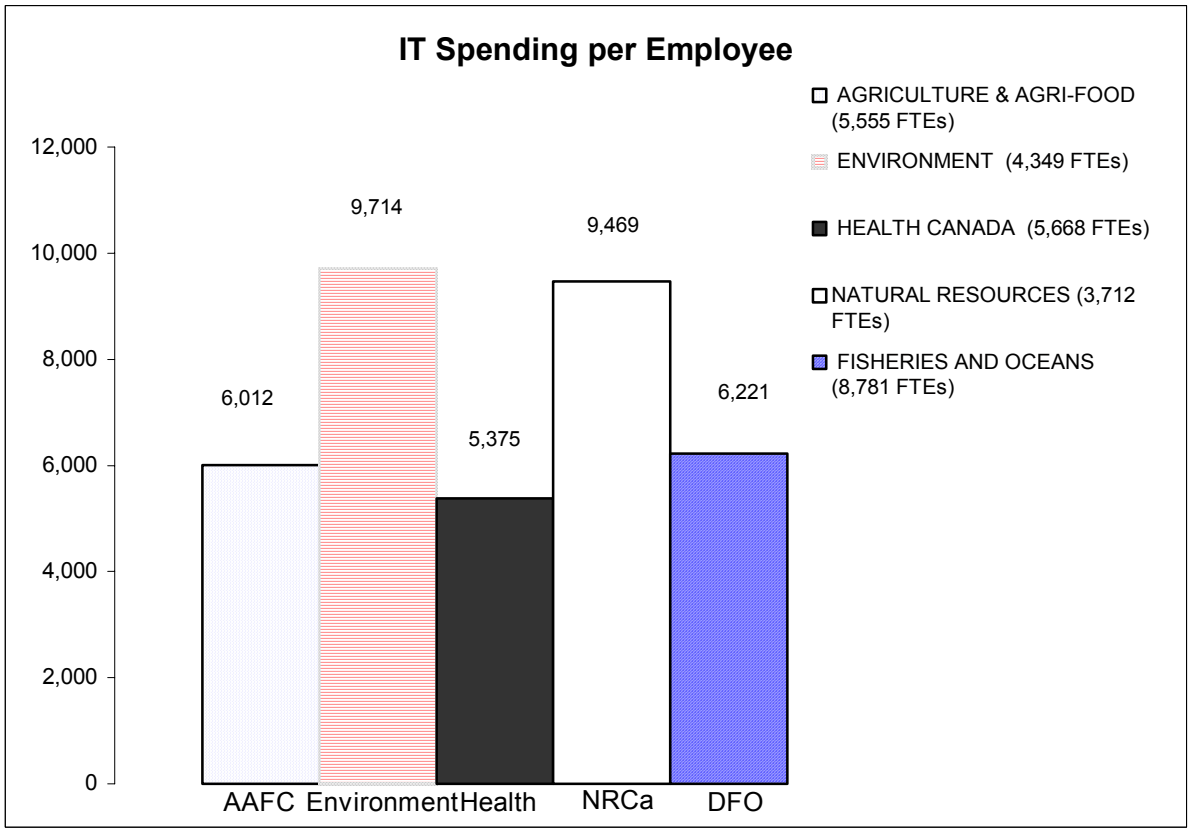
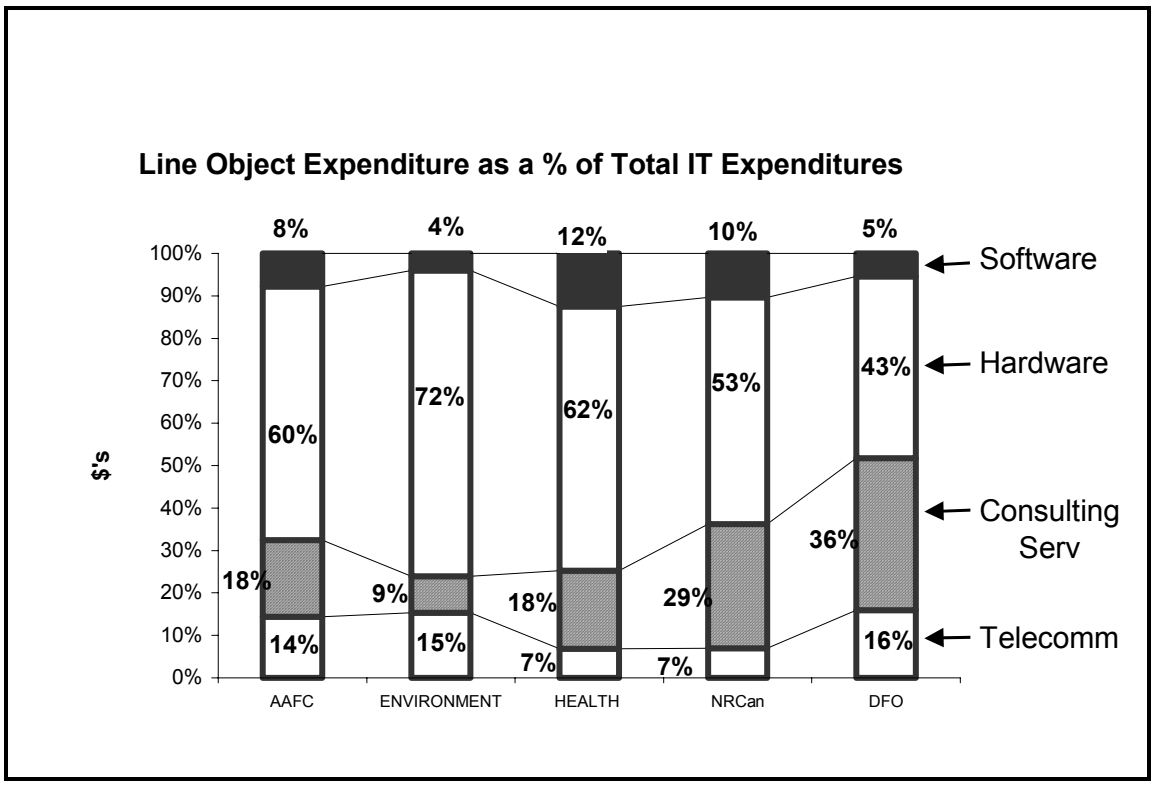


Exhibit 3.2.2.2 1997-98 IT Expenditures in Related Departments As A Per Cent of Base

Department	Per FTE Spending	Per Cent of Base
Health Canada	$5,375	2%
Agriculture and Agri-Food	$6,012	2%
DFO (TBS figure)[9]	$6,221[9]	4.8%[10]
Natural Resources Canada	$9,469	7%
Environment	$9,714	7.6%

[10] The Treasury Board Secretariat figures do not include salaries for DFO or for any other department, and this explains the difference between the DFO figure shown here and the overall expenditure per DFO FTE figure of $6,658 for DFO used in all other places in this report.

Exhibit 3.2.2.3 1997-98 IT Expenditures in Related Departments By Line Object Group



The foregoing analysis of expenditures showing percentage of total IT expenditures by line object groupings shows that there is significant variation in the manner in which IT monies are spent between the five departments. While DFO has the lowest spending on hardware, it spends more, on a percentage basis, than any of these other departments on consultants.

The following table shows "per FTE" expenditures for North American business, as well as governments at the federal, local and state governments in the United States. This table has been included as, during the discussion of the interim report at the Departmental Review Committee, a request was made to situate DFO's expenditures in a broader context, including the private sector. It is useful to note that notwithstanding the many weaknesses of this type of global comparison, DFO's spending per employee is on the same scale as that of business across North America. The table also shows that IT expenditures are heavily skewed and that while 50% of companies spend less than $7,000 per employee, this jumps to over $24,000 when 75% of the companies are added. This presumably reflects the level of reliance on IT for business purposes. The value of that information is to indicate that for those organizations that rely heavily on technology, costs per FTE can rise to a very high level. This is most apparent in the U.S. federal government where 50% spend less than $1,500 while 75% spend over $25,000, even more than comparable business expenditures. These global comparisons hold less value for DFO than the foregoing assessment of like Canadian federal departments, other than the observation that IT expenditures can rise dramatically (16 fold) between organizations with a moderate commitment to IT solutions and those with more aggressive implementations.

Exhibit 3.2.2.4 1997-98 IT Expenditures ($Can) in Government and Industry

Organization	25% spend less than this per employee	50% spend less than this per employee	75% spend less than this per employee	50% spend this per cent of overall expenditures
North American Business	$2,208	$6,996	$24,012	2.9%
U.S. State and Local Governments	$3,585	$11,481	$35,881	0.8%
U.S. Federal Government Departments	$810	$1,472	$25,636	1.7%
DFO actual spending is $6,658 per employee, which is 6.5% of total spending.				

The analysis of the Canadian Federal departments shows that IT represents a significant portion of departmental spending and is generally in line with the expenditures of the other federal natural resource departments. Projections of these expenditures into the future are difficult as there is a material difference in cost between a "stand pat" needs-based model and one which commits to aggressive implementation of IT in new areas. This report examines, among other things, how these expenditures are made across the department and the degree to which changes would be beneficial in terms of performance and value.

The most powerful way to eliminate duplication and inefficiencies is to consult, co-operate and consolidate with a view to achieving consistency. While there are organizations and approaches that can dramatically reduce costs (e.g., a high degree of central control, a short list of approved hardware and software), it is not clear that DFO's program needs and management traditions would support this approach. The strategy with the greatest probability of success is one in which there is genuine cooperation between clients and providers, as well as an appreciation of the benefits of consolidation. This model was found to exist, usually for specific projects or initiatives in Maritimes, Laurentian and Pacific Regions, and the NCR.

The department will realize tangible benefits from treating the network (including e-mail, an office "desktop" and user help) as a departmental asset. For this to be effective, this specialist group (IM/TS) needs to receive adequate funding not only to operate but also to maintain and evolve this activity. In several regions, there is a management model where "portfolio managers" are assigned by IM/TS to become experts in the needs of a particular business line. Where these positions existed, and links to the program areas were good, this was a "best practice" that did much to bring cooperation and consistency.

A key recommendation of the review can also be found in the 1994 Price Waterhouse report on IM/TS; specifically, "…end the practice of user chargeback for LAN management services. These services should be corporately funded." In order for this to occur, there must be a clear definition of what is and is not included, as well as an explicit and verifiable assessment of what level of funding should be provided. This recommendation is still a good one and its implementation would do much to address problems of inconsistency, inadequate levels of service in some areas

and the time and effort made chasing chargebacks. In order for this to occur, there must be a clear definition of what is and is not included as well as an assessment (possibly by the committee structure proposed in the "Recommendations" section of this report) of what level of funding should be provided.

The level of funding cannot be clearly set without agreement on whether to pursue a strategy of adequate support to program goals, or one in which DFO is on, or close to, the leading edge of the implementation of IT. There are substantial differences in the levels of risk and expenditures between being an efficient manager of IT and being on the "leading edge".

3.3 GOVERNANCE

3.3.1 Roles and Responsibilities

A key general finding, which occurred across all lines of enquiry, was an absence of effective implementation of relevant and meaningful policy. In some cases, this is an absence of a policy of any kind, while in others it is the absence of implementation of existing policies. The "who does what" and "how are things done" types of policy are the most important here.

The lack of such policies (lack of implementing of those that do exist) have resulted in a patchwork of approaches. This weakness has the largest impact on DFO's business in the area of custom and large-scale systems. The next most serious weakness is in the area of hardware and software acquisition. Another area where there is an absence of consistency is those services for which IM/TS is responsible in different regions. The presence or absence and level of chargebacks to programs is also inconsistent. Some regions keep high levels of IT expertise in program areas (e.g. Pacific), while others (e.g. Maritimes) have consciously moved staff from programs into IM/TS. There is even a middle ground (e.g. Laurentian) where some staff are funded by Science and are managed by Corporate Services. A number of important areas are identified in the report that will benefit from a higher level of consistency. This can be achieved through greater cooperation and consultation between program staff and staff in IM/TS. This cooperation, to provide all the benefits that are available, must be accompanied by clear agreements on where regional IM/TS and program coordinating committees can make binding recommendations governing expenditures and where their role is simply that of advisor.

3.3.2 Need for Client-Provider Consultative Approaches

In the 1993 and 1994 Price Waterhouse reports, there was a call for client-provider committees that would facilitate the use of IT. This requirement remains today. In any successful service relationship, the needs of the client must be the guiding force for the services rendered. There are two tiers: services that are provided without charge; and cost-recovered services. In discussions on the first tier, it is important for a mechanism to exist to ensure that requests are truly in line with needs. This mechanism could be that the evolution of core-funded services must be approved by all sectors, since sectors may need to accept lower levels of overall funding if new levels of service or services are deemed to be "core".

There currently are client-provider consultative mechanisms in various regions and sectors, but no definable pattern exists. At the regional level, we found some committees that had been struck for specific special projects. In a very few cases, region-wide multi-sector committees had been formed and in some cases members saw them as working well. There were also committees in which one sector would work with IM/TS on specific program needs. These were most apparent in Pacific, where IT resources can easily be identified as resident in programs.

At the national level, there was no client-provider committee structure during the period of the review. A committee made up of directors of IM/TS periodically invites those at lower levels in IM/TS, but these larger meetings occur only once or twice per year. A national client-provider committee (called the Departmental Informatics Working Committee) has not met for over a year, and appears to have been dissolved. In early 1999 the department established the Informatics Steering Committee (ISC) representing all parts of DFO. This committee will act as a steering committee for IT related matters. This is a beneficial step that can be the basis for resolution of several key issues identified in this review.

There is a clear need for at least two levels of national client/provider discussions. The first would be a high level forum with some of the responsibilities that have been proposed for the new ISC. This high level committee, to be effective, needs to be supported by other structures that are more able to address detailed and sector or region specific issues. These other structures/committees could consider how the department should address emerging uses that place significant new demands on the WAN/LAN than simple e-mail and text sharing. There are several cases now (including INNAV and multimedia) which, if implemented, would have the ability to stress the network's current capacity. The committees and working groups that support the ISC could focus on long-term strategic uses of IT. These uses are almost limitless, and there is a need to link program needs and desires with cost factors, technical feasibility and desirability. Given the costs and complexity associated with large scale use of IT based solutions (as shown in the expenditure data in the previous section demonstrating a rapid rise in expenditures between average, and above average organizations) it is important that "pilot projects" are well-designed and the results are widely shared. This is done on a very small scale now by a few sectors, but there is no large-scale sharing of experiences and ideas.

DFO could also benefit significantly from a user-provider updating of the informatics architecture standard. The creation of the DFO Informatics Architecture document and the subsequent infrastructure initiatives which were implemented pursuant to that document have dramatically improved the technical interoperability of the network and its systems. Issues remain, however, regarding planning, funding and managing the assets so that they function effectively to support the department's needs efficiently.

The recently completed Review of Corporate Services Redesign, in the area of IM/TS, indicated that clients emphasized the need to consult with departmental managers. The analysis conducted in support of the Review of the Management of Information Technology suggests that there is also a strong need for program managers to consult with IM/TS staff in a wide range of areas. The most important of these areas is large scale computer based systems, and custom software applications. It is also clear, however, that even day to day issues could be better coordinated and more effective if the management of information technology was based on integrated approaches. Large and

complex initiatives, in order to be successful, should be developed and implemented with input from IM/TS, and in a way that is compatible with departmental approaches.

3.3.3 Large-Scale Systems

A study of existing large-scale systems in DFO was undertaken to measure implicit and explicit management structures in relation to large-scale systems that represent significant IT expenditures. This element of the review looked at large scale systems in the NCR and one Region (Maritimes). The purpose was to assess the management of these systems from conception to implementation or completion (where possible). Large-scale systems were defined as custom systems costing more than $500,000, delivered to more than 100 employees or implemented across multiple locations.

There is no single approach used within DFO for developing and implementing large-scale systems. In the public and private sectors, there are several planning and development models that have commonly proven to be effective in both controlling costs and bringing desired results. At least two of the DFO systems which this review looked at grew from an anticipated cost of less than $100,000 to an as-delivered cost of over $1 million (Departmental Violations Information System and the Habitat Referrals Tracking System). Overall, those that were developed through project-specific teams that included staff from IM/TS as well as program staff, end users of the system and consultants (where appropriate), tended to work the best. In other words, they were developed in harmony with the technical architecture and recognized and addressed the needs of the final user. Where detailed plans were absent, including specific milestones and clear descriptions of what a successful system would do, costs were high and in some cases deliverables did not appear in the year they were expected.

The infrastructure support of these large-scale systems as well as the evolution and maintenance of the systems themselves and user training must be addressed at the outset. In some cases, system support has been charged back to programs by IM/TS. When costs and levels of support were not explicitly agreed upon early in the process, discussions have been described as difficult.

When programs evolve very large systems, there is also a risk that they could implement networks which parallel the existing system. Certainly the existing Coast Guard inter-city digital circuits and the proposals associated with the INNAV project, from a hardware and architecture standpoint, are very similar to the WAN operated by IM/TS. GTIS is the supplier of inter-city links for the Coast Guard and IM/TS systems. In meetings with the review team, GTIS staff indicated that cost efficiencies could be achieved by consolidating the acquisition of these services. Clearly an assessment of potential savings from such consolidation is warranted. Indeed what travels through these systems and the fault tolerance of the activity are different and in while IM/TS buys services and Coast Guard leases digital circuits, however the hardware and inter-city links are in many cases similar, and the supplier is the same (GTIS).

In conclusion, a coordinated approach to the development and implementation of large-scale systems is a key improvement in governance which DFO should consider. These systems are not only costly but, in some cases, systems to do the same thing are being developed independently in different sectors and regions (e.g. fisheries management information and licensing systems). The advantages of using an integrated, client-centered approach include cost savings as well as more

robust solutions where experiences and approaches from one region or sector can be used to improve results in others.

3.3.4 Administration of the IM/TS WAN

This portion of the review looked at the management of the information "pipes" that carry information between buildings and cities. In computer parlance, the size of these pipes is called bandwidth and the usage is called load or bandwidth utilization. Like the pipe example, it is possible to "size" these links (the bigger, the more costly) and it is possible to fill them so full that the whole system slows and ultimately shuts down.

The links are made up of two general categories. The first of these is the WAN, which is managed and funded by NCR IM/TS. The LANs are the links managed by the regions from their regional headquarters. The complexity ranges from Central and Arctic, where all inter-city links are operated as WAN components, to the Pacific, Maritimes and Laurentian Regions where high capacity fibre optic and inter-city links are administered from the regional headquarters.

The IM/TS WAN, which links together 94 DFO computers (i.e., routers) across Canada, is the primary system for inter-city communication of departmental e-mail, desktop applications and data. The day-to-day administration of this network is contracted out to Public Works and Government Services Canada (PWGSC) Government Telecommunications and Informatics Services (GTIS) group. In 1998-1999, GTIS subcontracted management of the system to a local private firm called NUVO Networks.

Information surrounding the management process that resulted in GTIS' being awarded this contract suggests that customary procedures were not followed. Managers of regional LANs indicated that they were simply advised the service would be provided by GTIS, without input or consultations with the regional client organizations. The review team was advised that when the contract was awarded to GTIS, the DFO contract to manage 94 routers represented a doubling of GTIS' responsibility. The management of this award does not seem to reflect the type of consultation and coordination that is considered desirable. In addition, as noted below, there are several weaknesses in the current arrangements.

A review of the service level agreement for 1998-1999, as well as a series of interviews with DFO and GTIS staff, have demonstrated that there are weaknesses in the document. These include:

1. The services that GTIS must provide to DFO are not defined in detail, although there are direct references to network availability and action to solve specific problems.

2. GTIS measures its performance against the network availability criteria, but is under no obligation to report when the specified availability is not achieved. Furthermore, if the specified network availability is not met, there are no penalties or financial remedies for DFO. The network availability would seem, therefore, to represent a "target" rather than a standard. A more binding service level would clarify what exactly DFO is purchasing and what consequences or actions flow from a failure to provide this service level.

These arrangements result in DFO receiving daily, weekly and monthly reports from GTIS/NUVO. These reports are so general, they have no meaning to either GTIS or DFO staff. While the total failure of any particular link in the network is reported to NCR IM/TS if it cannot be repaired within two hours in the business day, total failures are far more rare than overloaded conditions that slow down all communications including e-mail and Abacus sessions.

In addition, the reporting is not stratified so that the six links that are critical for inter-regional communication are shown separately. The Vancouver WAN link, for example, supports all network communication within the Region and with other Regions. Its failure therefore affects all 2,344 staff in the Pacific Region and the ability of the rest of DFO to reach them. This is an entirely different situation than would occur if the link to a small sub-area office failed and only the few staff in that office would be affected. The daily reporting system currently provided by NUVO treats these two links in an identical way.

A detailed analysis of the architecture of the network was conducted. The nature of the management of the LAN and WAN made it difficult to identify all of the equipment connected to the LAN/WAN. After a comprehensive "topology" was prepared, it was clear that the DFO network reflects its history of having been assembled by linking together a variety of sub-components, rather than having been designed as a whole.

GTIS, who is responsible for making architecture recommendations as a part of the current service level agreement, has not done so. The computer consultant who conducted this component of the review has indicated that DFO could achieve cost savings in network management costs and increases in security and performance if a consolidated department wide architecture were implemented. The failure by GTIS to provide architectural recommendations that would support increased performance and decrease costs, that are required by contract, is seen by the review team as a serious shortcoming. As the contract contains no penalty provisions, there would appear to be little that can be done to remedy this until this work is re-tendered in the subsequent fiscal years.

The effective management of "bandwidth" is one of the most apparent measures of service to clients. When network links become overloaded, the time taken for information to travel across the network increases. This is especially evident to users when mission critical applications like Abacus, Peoplesoft and, in some regions, Word and Excel, are delivered from a central location. If e-mail takes a few minutes or a few seconds, it is seldom apparent to users; however, if a user is entering data or preparing a report and it takes minutes to get a response from the application, users become frustrated and application-related problems can result. As a result, one network management function is to watch the level of "traffic" on network links and ensure that the level of service is good under "normal" circumstances.

The reports currently provided by GTIS to DFO report on only the ten busiest links. In several cases, these are situations for which no remedy exists that would overcome slow or overloaded links, because the local telephone company has limited service to the area. In other cases where large inter-regional links become slow, there are no agreed-upon explicit steps to be followed. The current management of the WAN has three approaches that they use. An assessment of several examples has not demonstrated how one approach is chosen over another. The review team asked

for written guidelines which would apply to these management decisions and was told that none existed.

When links become so busy that performance degrades, the options are to do nothing, to increase the capacity of the link, or to prohibit certain applications from being used. The first approach was apparent in discussions with IM/TS staff where they have indicated that for some small DFO offices, although increased capacity is required, there is simply not enough money to purchase the equipment and services to accomplish this. As an example of the second strategy, the capacity of six WAN links was improved in October 1998, demonstrating that in certain circumstances increased capacity is purchased. An example of the last strategy related to actions taken in regard to the WAN link connecting the Newfoundland Region to the rest of DFO. In that case, Abacus users in Newfoundland found performance across the WAN to be slow. Rather than doing nothing or purchasing greater capacity, a decision was made to shut down multimedia access to all users in Newfoundland, NCR and Central and Arctic. There was no consultation with or notification to network users of this change. Further, when adjustments are made to redirect Newfoundland Internet traffic through a regional firewall, it is not clear whether this multimedia access for NCR and Central and Arctic users will be restored.

GTIS is identified as responsible for identifying network links that are overloaded, identifying remedies to DFO and implementing remedies. Even though the SLA clearly identifies this type of analysis as GTIS' role, DFO staff routinely conduct this analysis and all of the recent link upgrades have been implemented as a result of the work of DFO staff, not staff from GTIS.

3.3.5 The Need for IT Support Outside Of Normal Working Hours

DFO's programs, especially those relating to emergency response, must operate effectively at all times. While many "mission critical" activities rely on the WAN/LAN, the historic approaches of fax and telephone serve to "back up" these WAN/LAN approaches. As technology moves more and more into an essential role, this ability to use "the old way" will diminish in effectiveness, thereby increasing the need to reduce single points of failure in the WAN/LAN. During this review, program managers often expressed concern that the increased reliance by programs on IT infrastructure requires that the WAN/LAN deliver completely reliable performance 24 hours a day, 7 days a week.

Currently only 6 of DFO's 94 routers are supported on a 24 hour basis. All other routers on the WAN/LAN are supported during the business day only. The Coast Guard inter-city links, where the program mission requires it, are supported 24 hours a day. In order to implement any consolidation of the IT functions currently found in Coast Guard and IM/TS groups, it must be assured that the off hour business needs of clients are fully met.

The threat and risk assessments recommended in the security section of this report can be used to identify if there are current WAN/LAN elements beyond those already supported that require 24 hour support. It would appear that the high reliance on e-mail, especially during emergency response to spills, marine accidents, and fisheries enforcement activities would make the e-mail system a candidate for 24-hour support. It must be noted here that, because of the costs of paying staff for standby and call-backs, implementation of 24 hour support in all regions could be costly.

3.4 NEED FOR POLICIES

3.4.1 General Areas Where Improvement is Required

A key general finding, which occurred across all lines of enquiry, was the need for the implementation of "who does what" and "how are things done" types of policy. In some cases, the limitation is the absence of applicable policy; in others, it is failure to implement an existing policy.

The general areas in need of relevant and meaningful policy guidance that is in line with program needs and user input are as follows:

1. LAN/WAN level of service commitments;
2. security of LAN/WAN equipment, desktop devices and data on servers and local machines;
3. fault tolerance in the LAN/WAN and e-mail, including tolerance of single points of failure and the requirement for 24 hour support;
4. LAN/WAN level of service to small offices, and very remote sites including ships;
5. criteria for evolution of the desktop office suite including the e-mail system;
6. acceptable use of Internet including any differentiation between use during and outside of normal working hours, and the degree to which DFO will serve as a general Internet Service provider for its staff;
7. the use of modems configured to auto answer on desktop computers connected to the WAN;
8. conditions under which a LAN may be set up to meet program needs;
9. departmental Internet firewall rules;
10. location of all network devices and the provision of uninterruptable power and backup;
11. extent and nature of support outside of normal working hours;
12. allocation rules for accessing bandwidth including a definition of when bandwidth use will be charged back to program areas;
13. consistent salary treatment of time spent working on DFO business on a DFO-owned computer linked to the DFO network outside of business hours;
14. identification of compatible hand-held computing devices, supported platforms and supported uses;
15. identification of what information types are to be placed on the Internet, and Intranet, and what types of information are not to be published in this way; and
16. a clear identification of the types of information that can be distributed by mass e-mail, and circumstances and mechanisms to direct widely distributed e-mail only to employees for whom it is relevant.

The absence of clear advice and direction extends to acquisition of "off the shelf" hardware and software, as well as to custom system development. In the user survey conducted for this review, a question related to "resources considered while making a purchasing decision" allowed the identification of multiple resources. Only 30% of those with purchasing authority consulted the DFO Informatics Architecture document, Help Desk or IM/TS staff before making a purchase, 38% consulted reviews in computer magazines while 72% consulted a knowledgeable colleague.

In Maritimes and Laurentian Regions, there is strong pressure to use a robust planning process tailored to DFO's circumstances by DMR (a private computer consulting firm) before beginning a custom application development project. Even there, projects initiated in program areas often use only a portion of this DMR process.

The operation of the LAN/WAN system also exhibits wide variation in implementation and operation. As an example, in some regions, very tight control over Internet access can be contrasted with very few limitations in other regions. Similarly, there continue to be proposals to set up LANs and WANs entirely within program areas (e.g. INNAV, a recent Coast Guard initiative that is still under development). Should these proceed, the result would be that the same equipment running the same software, accomplishing the same "interlinking" objective would be done by two parallel organizations in the same department.

Even the serious training deficit identified by the user survey (40% of DFO staff want to have IT training, although the nature of the true need for training cannot be assessed by a survey) can be traced to the absence of a policy that calls for integrated implementation of new software and systems. This integration should include obligatory training as well as an assessment of network issues that may emerge. The recent partial roll-out of Office 97 has been associated with training issues (25% of DFO staff still want training on the desktop suite). It has also faced equipment compatibility issues. The Laurentian Region, presumably one of the main beneficiaries of the additional support for bilingual tools in Office 97, could offer Office 97 to only half of its users because of hardware limitations. Furthermore, the file incompatibility between Office 97 and its predecessor was identified by users as a major problem associated with this change in the desktop.

3.4.2 Want vs. Need

Microsoft's marketing department ensures that almost everyone in North America recognizes the phrase "where do you want to go today". In a business-computing context, however, a more relevant credo is where do you ***need*** to go today. DFO demonstrates the implementation of both models, the former being the more expensive, the latter being more appropriate in this time of temperate spending. The 1994 Price Waterhouse review of IM/TS clearly stated that "the solution [to too many half-done or unstarted projects] should be to do less, rather than continue to juggle conflicting resource demands".

DFO, through the Informatics Architecture process, undertook a comprehensive and necessary harmonization of hardware and software. If time had stood still, this would have been almost all that was needed. We began with a "work group" environment (where small groups of employees shared information among themselves and chose different word processors, operating systems and e-mail systems). We have now moved to a "fully integrated" model (where communication across the department is facilitated through a desktop standard for file sharing, a single network operating system and a single e-mail system.)

The cost-effectiveness of PC computing over almost any other product group came about solely as a result of strong standards. When the public chose to see the IBM desktop system as a standard in a "Tower of Babel" environment, PC computing exploded. In less than twenty years, sales of desktop computers have gone from zero to 200 million units per year. As Bill Gates noted in his

testimony in 1998 before the U.S. Senate in response to the Senate's assertion that Microsoft had operated in monopolistic ways, if aircraft costs and performance had followed the same price-performance curve as computing, "a 747 would cost as little as a pizza". Standards have been the key to efficiency and price competition, and offer DFO the opportunity to be efficient and cost effective in the area of IT.

The key question is how standards should be set for DFO that would be driven by clear program needs and the financial constraints that we face. It may be useful for us to consider what is necessary first and what may be desirable later. DFO could benefit significantly from a user-provider evolution of the Informatics Architecture standard. We are now in an environment that includes palm computers, worldwide digital satellite communication and sophisticated implementations of multimedia. None of these are considered in the architecture document but all now exist in various forms within DFO.

3.4.3 Evolution Of The Standard Office Suite

As a part of the Informatics Architecture process, a decision was taken to move to the Microsoft Office suite of products. This decision was made through a process that not only accounted for hardware compatibility but also included consultation with clients across all sectors. As noted elsewhere in this report this approach is considered to be a "best practice".

The next Canada-wide modification to the standard desktop was handled differently. In 1998, the desktop suite was upgraded from Office 4.3 to Office 97. This new version was purchased as DFO's national standard even though a business case had not been prepared showing the incremental benefits, and inventory information showed that a substantial number of users would be unable to move to the new standard because of limited PC memory and slow processors. In addition clients were not consulted on the need for any increased capability that Office 97 might bring. Only those users that had sufficiently fast computers were given Office 97, which left those operating Office 4.3 with file incompatibility problems with other DFO users. The current assessment that Office 97 does not run adequately on 486 machines, coupled with the cost associated with upgrading the hardware, suggests that this situation will remain until all of these machines are replaced. During interviews and discussions there were frequent reports of DFO staff receiving incompatible Word, Excel and PowerPoint files. An interim solution for management of this IT incompatibility problem exists and should be implemented.

A return to the business case model utilized in the development of the Informatics Architecture document is important, as Microsoft is continuing to evolve their desktop office suite and the pre-release version of Office 2000 is now being sold to the public. DFO must ensure that future changes to the departmental desktop are done only after a full business case is developed. Office 2000 moves all key office functions into the Internet paradigm. Every computer in the network can "publish" documents, reports spreadsheets and presentations as Web pages. This is clearly a major change and should be subject to a full business case analysis including user needs, hardware and security implications.

There may be situations where the group of individuals working on documents together uses a different document standard than the standard for DFO. This is often the case in Science where

collaborators are commonly from other scientific institutions. This is a likely explanation for the survey results which indicate that Lotus Word Pro and WordPerfect are found on some DFO machines. Clearly any departmental approach that is based on interoperability would recognize that within DFO the DFO standard would apply, and where other standards were appropriate, that DFO staff, in order to achieve a meaningful level of interoperability with collaborators, would have to have access to other desktop products, or other versions of the Microsoft products.

3.4.4 Internet – "Where Can I Go Today"

In this review, new IT-based approaches have been contrasted with the older "low tech" approaches to assess the management of the new against the management of the old. This is very difficult with respect to the Internet. Throughout this section, all references will be to Internet, not the internal government system called the Intranet. While the Intranet bears many similarities to its giant cousin the Internet, from a security standpoint they are worlds apart.

At the outset, it is important to note that we were unable to find an analysis or business case discussing the provision of full Internet access for all departmental employees. There are other federal institutions as large or larger than DFO (e.g. Revenue) where full Internet access is not provided to all staff. Certainly some DFO users, most often in Science, have been using the Internet since its inception.

In some ways, the "non IT" equivalent of the Internet is a library. The Internet has direct or indirect access to all kinds of information. It is instantaneous and anonymous and also is bi-directional. Furthermore, it is possible for individual Web sites to determine who has visited them and to find out technical information about visitors' computers. On the other hand, when employees visit a DFO library (the only generally available information source DFO provided for its staff prior to the existence of the Internet), they find that there is a carefully selected array of resources that relate to DFO's business as well as general sources of information including newspapers. In providing Internet access to all users in DFO, a far broader range of resources has been made available.

The Treasury Board Secretariat (TBS) is aware of this broad range of resources and has developed a high-level Acceptable Use Policy, which includes a recommendation that individual departments develop matching policies that relate more specifically to their situations. This policy calls for routine audits of departmental implementation. DFO has yet to conduct such an audit.

In the absence of an approved departmental policy, DFO has not monitored which Internet sites are being visited. Furthermore, while it is possible to "block" access to sites, at the moment only three of the firewalls have such blocking enabled. In all cases, the only use that is blocked is multimedia audio and video. This choice appears to be in conflict, however, with the transition of the departmental desktop standard to computers with sound cards and speakers, which provide the benefits of sound as an adjunct to the operation of the computers. In three regions and NCR, where this multimedia blocking has been implemented, users were not notified that the change was occurring (the fourth region with such blocking, Laurentian, advised all users of this change). The choice was made in the full knowledge that some remote DFO offices in the North would be blocked from their only access to CBC radio and that certain staff in the NCR were monitoring

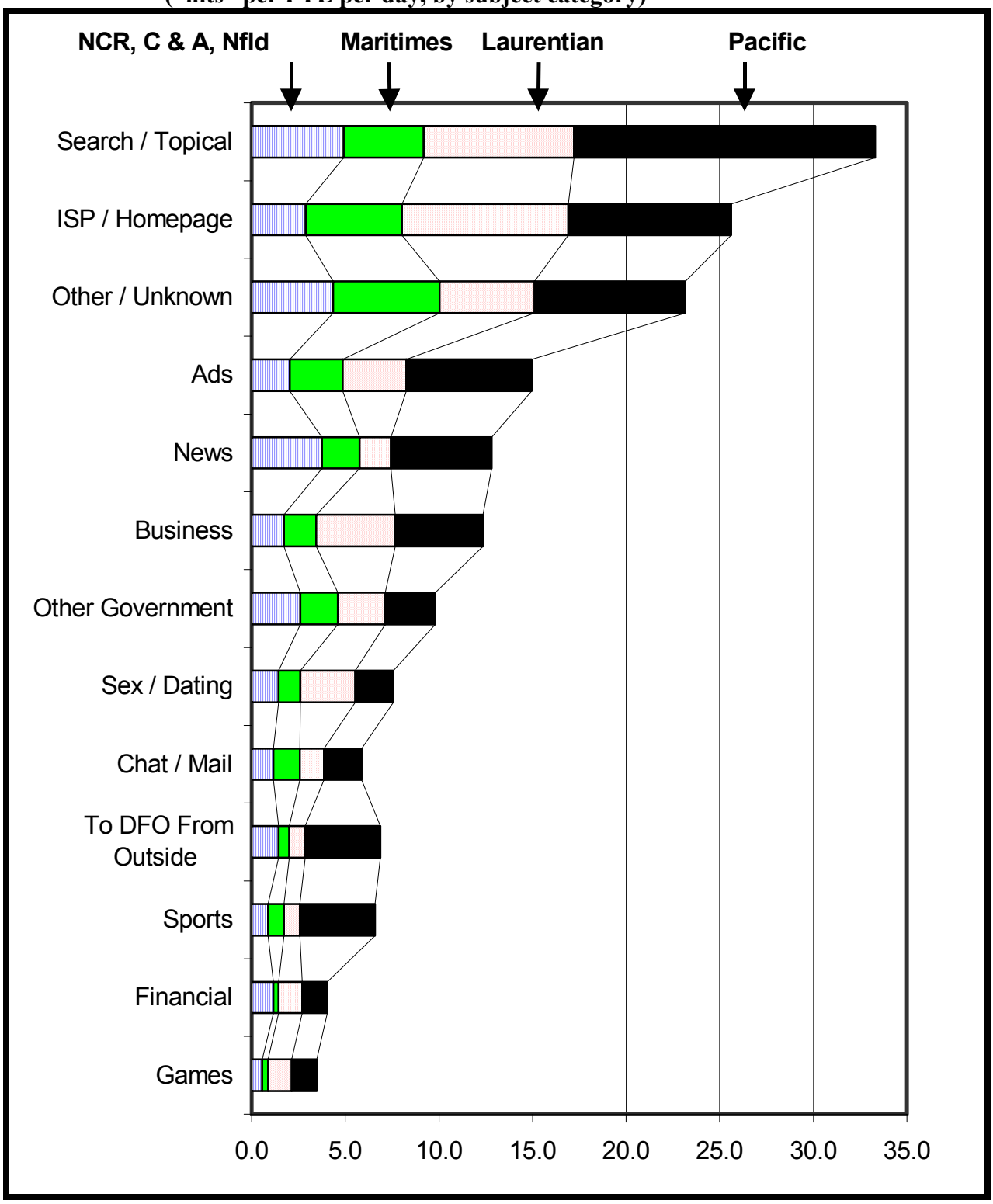
local radio in coastal communities. This blocking was done to reduce load on the network ("bandwidth") links between Newfoundland and NCR, while other network traffic to sites that are clearly unrelated to DFO's business remain open.

There is a further Internet inconsistency. While all DFO users have access to the Internet from their desktop, users in Maritimes who access the DFO computer from remote locations are given full access to all departmental resources, including the Intranet; however, Internet access is completely blocked (unless a specific use agreement is signed). Staff in NCR were subject to this limitation until the spring of 1999, when full Internet access was provided to remote users. No notice to users was made when this access was originally blocked and no notice to users was given when this full access to Internet was restored. DFO staff in Newfoundland, Central and Arctic and Pacific Regions who dial in to the DFO network have full Internet access. There is no policy basis for this difference. There is some concern that DFO staff dialing in from their homes would use DFO in the same way one would use a commercial Internet service provider. At the time of the review there was no DFO policy indicating that such use is unacceptable. An Acceptable Use Policy was issued on May 28, 1999 but is silent on remote access to Internet using DFO dial up lines.

A comprehensive analysis of Internet use by DFO staff in all regions shows that at least 10% of Internet traffic is to sites that are clearly not work-related. For each of the department's four firewalls that handle Internet access, the use was divided into 13 categories. The categories and their definitions are shown below.

To DFO From Outside	A DFO site: Coast Guard, Institute of Ocean Sciences etc. As this is firewall traffic, only incoming traffic from outside is shown here. Visits by DFO staff to the DFO Intranet can only be monitored on the 30 Web servers currently in use for this.
Other Government.	Other federal and provincial sites: National Research Council, HRDC
Search / Topical	Search and starting point sites: AltaVista, MSN
Business	Business related sites: Cambridge Scientific, ZiffNet
News	News sources: Canoe, newspaper sites
Financial	Financial sites: Banking sites, stock market sites
Chat/ Mail	Chat and Mail sites: Hotmail, Yahoo Chat
Ads	Ad sites: double click
Sports	Sports information sites: NHL sites, football and baseball sites
Sex / Dating	Sex and Dating sites: US Date, liveteen.com
Games	Game sites: Computer and other games; Sony Playstation site
ISP / Homepage	These represent user or other homepages such that the actual site visited can not be determined as many sites are hosted there. The ISP "Geocities" figures prominently, which is a site where music (MP3) files are found.
Other / Unknown	Sites where content could not be determined; no reverse lookup and / or the root page does not contain any site information or links. Eg: 209.143.228.181

Exhibit 3.4.4.1 One Week of Internet Traffic By Firewall
("hits" per FTE per day, by subject category)



This graph clearly shows that visits to government sites is low, when compared to generalized searches and "unknowns" (sites operated by the federal and provincial governments will, for technical reasons, not occur in this category). They also show that approximately 10% of the traffic is to sites with no apparent business purpose The actual average use of Internet was assessed as average number of Internet responses ("hits") per FTE per day. These are shown on the following table.

Region	**Internet Hits per FTE per day**
Maritimes	28.5
Newfoundland	28.9
NCR	
Central and Arctic	
Laurentian	42.2
Pacific	67.0

It should be noted that while users who dial-in from home in NCR and Maritimes have no Internet access, users that dial-in from their homes in Pacific, Laurentian and Newfoundland Regions have full access to the Internet. As the WAN/LAN and firewalls show low level of usage outside of normal business hours, and as Internet access is charged to DFO on a flat rate basis, it is not possible to identify costs associated with the use of Internet by users dialing in from their homes. One potential cost would be if additional dial-in "ports" were required to provide this Internet access from home. Pacific Region has half as many dial-in ports per FTE as the NCR, with twice the overall Internet use, so there is no evidence that additional dial-in ports have been installed to provide Internet access to DFO users from their home computers. The Acceptable Use of Policy issued on May 28, 1999, makes no differentiation between Internet use regardless of whether the connection is from the desktop or by dial-in.

The expenditures directly associated with the provision of Internet access are low when compared to departmental expenditures overall. It should be noted, however, that the "clogging up" of the WAN link between DFO and the rest of the department was, according the IM/TS staff, caused by extensive use of the Internet, and this use was characterized as related to the impeachment proceedings in the US. It is therefore important to note that Internet access across the DFO WAN/LAN can be a cost factor. The use of "non business related" sites either during or after hours was not a significant cost factor during the period which was monitored for this review. There would seem, however, to be management (salary/workload) issues which relate to overall productivity in the department. During the conduct of this assessment, no criminal use of the Internet was detected.

3.4.5 Access from Remote Locations

DFO requires remote connectivity for various purposes, including secure access from field offices, ships, teleworkers working from home, staff on travel status who need to access e-mail services and employees working from home outside working hours. As indicated in the user survey, approximately 2,520 people access the DFO network from outside the office. Of this group, 650 people access the network from a DFO-owned home computer.

The user survey indicated that 65% of remote access users were satisfied with their remote access and 62% felt that such remote access was reliable. Overall, while the difference is small, respondents rated the ease of use of remote access slightly more favourably than the reliability of the connection/access software. The average rating for ease of use, using a 5-point scale, was 3.84, compared to an average rating of 3.71 for reliability. In general, these are positive ratings, indicating that remote access is generally working well. On average, Pacific Region respondents rated reliability the lowest. Fisheries Management and Science rated ease of use the lowest and Fisheries Management also rated reliability the lowest.

Remote access is delivered differently from region to region. Connectivity and speed of remote access varies tremendously nationally and within regions. There is no policy on who may or may not have (high capacity) Integrated Services Digital Network (ISDN) or digital lines; it is at the discretion of IM/TS, even if IM/TS does not fund these lines. A review of the management practices governing remote access found that record-keeping is unreliable. In some cases, staff were required to complete forms, while in other cases no paper or electronic authorization exists. Cross matching of actual records of remote access for one month against the approval forms confirmed that the management of this is uneven and controls are not visible. As was noted in the section on Internet access, there is inconsistent treatment of Internet access from remote locations. Policies, procedures, roles and responsibilities for remote access need to be clarified.

The management of IT as it relates to DFO-owned desktop computers in homes of the staff are also uneven. As noted above, the user survey indicated that approximately 650 people work after hours from home on DFO-owned computers. A review of the dial up user documentation could not identify that any of these individuals had entered into a telework agreement with DFO. A general management issue caused by IT is the differential treatment of overtime from these home computers. It is not clear if the provision of a DFO-owned (non-surplus) computer to a staff member constitutes implicit "authorization" of overtime or some form of employee benefit. It is not clear that DFO-owned home desktops are some form of (paid or unpaid) teleworking.

There is very little explicit implementation of "teleworking" where individual employees forego an office and conduct their work for the department during normal working hours from their homes. The few "teleworkers" now in place are generally utilizing this approach in response to health-related concerns, and for periods of less than one year. Given the funding pressures on the department as well as the flexibility which teleworking provides (where no formal office space exists for the teleworking staff member), a clearer management of this IT-created opportunity is desirable.

3.5 SECURITY

3.5.1 Threat and Risk Assessment

During the conduct of this study, the Coast Guard commissioned a study of secure network communications. While the scope of the study was restricted to the Coast Guard sector, and much of the analysis was inferential, this study and its threat and risk assessment provide a useful indication of the nature and impact of threats that exist for the DFO WAN/LAN system. The

results of the Coast Guard's study was provided to the consultant conducting the analysis of the WAN/LAN for this review. Taken together several key areas for action have been identified. Specific areas of risk that require urgent attention are identified in the following subsections.

3.5.1.1 Architecture of Internet Links

An important priority has been assigned to Year 2000 compliance to ensure that critical DFO systems remain operational. However, it is equally important to ensure that our network is secure from other more current threats as well, especially from the Internet. Analysis suggests that some serious threats may exist from the manner in which access to and from the Internet is configured. While the Internet has provided quick access to a wide variety of information services, and enabled written communication (e-mail) to be as fast and as universal as the telephone, it is a very hazardous environment. Our interfaces with it (Internet firewalls) are managed unevenly and without the benefit of clear policies and rules. The net effect of this is that there are "more permissive" and "less permissive" sets of rules governing Internet traffic. The nature of a WAN/LAN is such that the least permissive firewall sets the level of risk for the entire system, even though there are six firewalls in DFO. Effective management of this aspect of IT again calls for a "business case" approach, as it does elsewhere. Certainly there are users that are accustomed to largely unfettered exchanges with outside users across the Internet. Such a business case analysis will assess how best to support real needs in a way that limits threats to the entire network.

The architecture of the electronic mail system was also identified as one with a high exposure to risk from Internet. The current system has some implementations where all mail, regardless of origin, is sent to mail servers that are inside the firewall system. On the Internet there are simple and readily accessible tools that can act as "mail bombs" and shut down entire-mail servers. If mail coming from the Internet was handled by a separate server (usually outside the protected area), then DFO internal mail could survive an Internet based attack. In some regions (e.g. Maritimes) the firewall is operated in such a way that problem mail (i.e. relaying of junk mail) is stopped at the firewall. This approach is not implemented on the NCR firewall, which passes all mail, including mail that calls for relaying.

In order for DFO to ensure its ability to conduct electronic business without interruption, the review recommends that a detailed threat and risk assessment be conducted specifically on Internet access and the configuration of the e-mail systems.

3.5.1.2 Protected and Sensitive Information

This review found no routine program that informed users of the security level of stored electronic information and electronic mail. The survey conducted as a part of this review indicated that of all shared services, the most valued is electronic mail. In many key areas, electronic mail has completely replaced the paper mail system for communications within DFO. While no study of the contents of electronic mail or electronic files was conducted, there is a risk that if not secret, certainly sensitive information (enforcement actions, personnel information etc.,) exists as electronic records in the DFO system. During the conduct of the review, the Coast Guard

commissioned an extensive security study which found that the current mail system can be intercepted and modified.

The management of the use of electronic mail, now that it is the most common communication system in the department, requires that a full threat and risk assessment be conducted. While no evidence was found that Secret or Top Secret information was being sent in e-mail, certainly sensitive departmental information was being sent. The four categories for sensitivity of information are:

1) Very Low - That information, if compromised, could be expected to cause no injury outside the national interest (UNCLASSIFIED);

2) Low -That information, if compromised, could be expected to cause injury outside the national interest (PROTECTED A);

3) Medium - That information, if compromised, could be expected to cause serious injury outside the national interest (PROTECTED B); and

4) High - That Information, if compromised, could be expected to cause exceptionally grave injury outside the national interest (PROTECTED C) and information that, if compromised, could be expected to cause injury to the national interest (CLASSIFIED).

The consultant retained by the Review Directorate for this portion of the work assessed that our network was secure up to the Protected A level, as it was designed to be. While a further study could address this issue in more detail, during discussions with DFO staff it became apparent that there was no understanding of the "limit" to the sensitivity of information that could be sent electronically. There is reason to believe that information characterized as Protected B (which includes information that could be embarrassing to the department or sensitive information about DFO operations, staff or programs) is being transmitted over the current email system. While there are technical solutions (see 3.5.3 and 3.5.4 of this report) they are costly and would take time. A valuable first step would be to advise staff that electronic mail should not be used for the transmission of sensitive information. This would include, for example, e-mail which contained credit card numbers and the name of the authorized user of that card.

3.5.1.3 Access by Non-DFO Staff

The DFO WAN/LAN has three distinct groups of "non-DFO" users. The first are contractors and students and others who, during their tenure with DFO, are provided with user names and the types of access specified by the DFO supervisor or client. The primary risk here relates to closure of these accounts when this access is no longer appropriate.

The second group are federal employees of other departments who are located in DFO buildings. The department with the greatest presence is NRCan although Agriculture and Agri-Food staff also have access. The Natural Resources Canada (NRCan) staff are, for the most part, located in the Bedford Institute of Oceanography and the Institute of Ocean Sciences. At the Bedford

Institute, their desire for a more open exchange with the Internet than the Maritimes IM/TS permits has been resolved with the NRCan staff having their own Internet access and no access to the DFO WAN/LAN. At the Institute of Ocean Sciences , however, permissive firewall rule changes have been made which bring some risk to the WAN/LAN. If staff from other federal departments find that they need a level of access broader than DFO permits for its own staff, then clearly a business case should be made, and the risks and benefits need to be explicitly assessed. The review found no such business cases during this review.

The third group of non DFO users can be found at the Canadian Coast Guard College. The College is now training staff from countries around the world. In the course of their work they utilize the department's IT infrastructure both in supervised classrooms and in unsupervised situations in common areas and their residences. While there is a firewall between the Coast Guard College and the DFO WAN/LAN, it is currently used to limit traffic from the DFO WAN going into the College, rather than being used to limit access from within the College. The Coast Guard College also operates an Internet firewall and has implemented rules that allow unlimited access out but severely restricts incoming traffic. In addition, the architecture of the Coast Guard College e-mail implementation is conservative and resistant to some of the risks that are evident in other parts of the WAN/LAN. The rationale given for implementing a firewall between the Coast Guard College and the rest of DFO was that the current DFO WAN/LAN did not provide adequate security from tampering.

3.5.1.4 Auto Answer Modems

DFO staff have used computers in their homes to conduct the work of the department for some time. Prior to well established networks and the type of high speed telephone access now available, DFO staff who wished to work from their homes could telephone to their office computer from a computer in their home (or other remote location like a field station or a hotel) and connect the two computers directly. This was done through a device called a modem (**mo**dulator/**dem**odulator) which allowed the DFO desktop machine to "answer" the incoming call and give the remote user access to their own machine as well as the DFO Network. In the current environment with reliable high speed dial-up access and Internet electronic mail, the requirement for these modems is reduced. Nonetheless, where these modems are left on after work hours, and have inadequate security systems in place, they can represent a way for unauthorized users to gain access to the entire DFO WAN/LAN. While configurations do exist (e.g., dial back, where the modem calls out to a single phone number known to be the users authorized location), there is no policy to require this type of configuration.

In order to manage this IT based risk a simple test can be conducted. A first step to identifying the degree to which such "auto answer" modems exist on DFO phone lines would be to "sweep" all DFO lines during the silent hours and identify which lines respond with an electronic handshake. When this list of "answering" phone lines has been created, and fax machines have been removed, the users of this type of "dial-in access" can be identified, and steps can be taken to ensure that adequate security is in place. At a recent meeting of the Institute of Internal Auditors, these auto answer modems were identified as the most serious security risk to the banking system worldwide.

3.5.2 Physical Security of Assets and Information

Securing IT assets physically is identical to the process used for other valuable assets in the department. One peculiarity is that computers (including servers and workstations) can almost immediately be broken up into components that are indistinguishable from newly made components. Another more important aspect is that the information that resides on the computer may be lost forever if it is not "backed up" to tape or the network. There is a further risk for those computers which play a significant networking role (servers, routers, name servers etc.) that contain information that would be useful to those trying to "break in" to the DFO WAN/LAN.

DFO has lost information and computers due to conventional theft. In one case, a departmental employee, upon leaving DFO, took a computer tape of catch data, which he used as the basis for opening a consulting business. Based on prevailing copyright law at the time, the only crime, as it turned out, was the theft of the tape itself, which was valued at less than $50. In other cases, desktop computers and memory inside the computers have been stolen. Security staff have noted that, while the theft of computer memory chips was a serious problem three years ago, it no longer is. This is attributed to decreases in computer memory costs rather than any change to physical security. When DFO offices have been occupied by protesters, there also have been cases where computers were damaged or destroyed.

Most LAN and WAN equipment is secured in computer rooms with combination locks. While this seems secure, often the walls of the room are drywall and can be easily removed. Most major DFO offices have video monitoring of entrances and exits. While this does not prevent theft, it may deter some thieves. In 1996, the server room at another Government department (the Journal Towers situated across from DFO headquarters at 200 Kent Street) was completely emptied of equipment in less than two minutes with full video coverage; however, no one was ever caught.

There is merit in concentrating network machines in areas with not only good physical security but also appropriate back-up power, cooling systems, and fire suppression. Given the nature of network computing and the general reliability of the telephone system (over which even "internal" network traffic travels), it would be possible to locate all "mission critical" LAN/WAN equipment in fewer physical locations than is now the case. In several cases, program areas (e.g., Coast Guard, Science) have their own computer rooms as well. There is merit in assessing where cost savings or improved reliability could flow from a reduction in the number of locations.

Currently, strong physical security of desktop machines (e.g., cabling them to desks; using more expensive case locks) does not seem warranted. Laptops represent a potential for loss of equipment or data for those who travel, but the review did not uncover any evidence that this currently is a serious problem in DFO.

3.5.3 Secure Authentication, Encryption and Public Key Infrastructure (PKI)

Currently DFO is assessing the need for IT solutions that would ensure that e-mail can be proven to have come from the apparent sender, and ways to prevent knowing the contents of or tampering with electronic information on the WAN/LAN.

As a business case for this has not yet been developed, it is sufficient to note that the only concerns expressed by Treasury Board Secretariat relate to securing transactions conducted pursuant to the *Financial Administration Act*.

The paper system that we now have has the capacity to meet TB's requirements as long as the transactions remain on paper. Furthermore, as long as remote access is by dial-up into DFO devices, the security risks of the Internet are avoided. While the implementation of secure authentication and encryption tools is an inevitable step, it can be entered into slowly enough to allow for a full analysis. A Revenue Canada analysis of options shows choices ranging in price for the first five years (based on 30,000 users) from
$3.2 million to $10.1 million.

Corporate Services IM/TS staff in Laurentian Region have looked into this in the DFO context and may have helpful experience from which the entire department can benefit.

3.5.6 Security and Internet - Firewalls

The Internet is bi-directional (i.e., we can get information from the outside and, under certain conditions, others can get inside if not prevented). As a result, we need a "gatekeeper". We use a "firewall" which is a mechanism used to protect the DFO network from unwelcome visitors, as well as to keep records on the information passing in each direction. The firewall basically is a sophisticated computer that uses specific software to conduct these gatekeeping functions.

Firewalls govern what activities can pass through with the ability to allow certain things "out but not in" and the reverse. In a system where several firewalls play a gatekeeping role to the same system, it would seem to be important that they are managed according to a standard approach. The department has six firewalls (Maritimes, Laurentian, Newfoundland, NCR[11] and Pacific Regions and the Coast Guard College). Three of these (Newfoundland, NCR and Pacific) are managed from Ottawa through a contract with GTIS and the other two are managed regionally. The Coast Guard college manages their own. None of the firewalls has the same rules and there is no handbook or policy to govern what should be done.

How these rules are managed coupled with how "servers" are managed within the department is important. Twice in 1998, Science servers have been "taken over" by an individual from outside of government who used them to send up to 33,000 pieces of Internet junk mail per day (colourfully referred to as "Spam", after the luncheon meat of the same name). On the days that this occurred, it represented over 50% of the traffic on the firewall. Furthermore, in November 1998, an individual obtained broader unauthorized access to DFO systems and unsuccessfully issued instructions to DFO devices 300 times in one day. Firewall records indicate that attempts to enter our system without authorization are continuing. A management issue exists here as GTIS agrees that it is their responsibility to look for indications of Internet based attacks (called "probes") and to take action: however, they indicated that this is not being done. Pacific Region IM/TS staff discovered probing in the fall of 1998 and identified and took the necessary steps to ensure that these particular probes would be unsuccessful.

[11] Internet traffic from Central and Arctic, as well as for Newfoundland non-Science users, travels through the NCR firewall.

The implications are clear. In the spamming incidents, an unauthorized user gained access and issued instructions to a DFO device to send junk mail. Once inside the firewall, other more harmful results could have happened (e.g., changing or erasing data, access to other open servers in any region, installing a program that could look into e-mail messages, etc.). These harmful results are inevitable unless some important steps are taken. These steps include a threat and risk assessment, a clear statement regarding the level of risk to the system that can be tolerated and a suitable approach to limit risk where stringent access cannot be implemented for program reasons. The costs to the department will vary based on the level of risk and the acceptable amount of time certain functions like e-mail or an inter-city link can be out of service.

The department clearly needs general agreement as to how these firewalls are configured. A review of the change requests to firewall rules also points out that the system for rule changes is uneven. For two of the firewalls (Newfoundland and NCR), there is no audit trail within DFO to verify that the contractor (GTIS in these cases) has complied with requests. There are also three different firewall systems in place and even the three firewalls using the same software are each using different versions. This makes the day-to-day management as well as coordination among the firewalls very complex. There is a plan to move all firewalls to the same system, but this has not yet been done. There is also a move to have all six firewalls managed centrally; however, if there are standard policies and approaches, there is no technical need to eliminate the regional management of regional firewalls. It should be noted that when information on firewall rules was requested, the regional firewall managers in Laurentian and Maritimes were able to respond in one day while GTIS took over four weeks to respond to the identical request. This is another example of poor performance for which the 1998-99 contract provided no remedy.

While there are some needs (e.g., in Science) to collaborate openly with specific colleagues outside DFO, where such collaboration brings risks to the LAN/WAN, it must be assessed more broadly. The option exists for such machines to operate separately from the LAN/WAN or to implement an approach such as PKI. In some cases, it may be that this collaboration can be accomplished in a way that eliminates risk to the network as a whole.

3.6.7 Elimination of Single Points of Failure for Critical Systems

The heavy reliance by programs on IT for support is moving DFO to a position where the failure, for even a few hours, of inter-office or inter-city communications or access to core applications (e.g., e-mail) can cause serious disruption. A concerted effort to ensure that core functions are identified and that single points of failure in these systems are eliminated is critical in ensuring that key departmental roles (e.g., search and rescue, oil spill trajectory monitoring, etc.) are available at all times. Where merged administration of Coast Guard systems is considered, it is critical to note that many of their navigation and search and rescue functions cannot tolerate failure. This is very different than general e-mail, word processing and financial functions where a 24-hour delay can often be tolerated.

Recently regional IM/TS staff at the technical level have struck a working group to help find solutions in many of the foregoing technical areas. This is a valuable step and with the inclusion of

IM/TS NCR staff and representatives of clients, simple workable solutions may be found in these and other important areas.

3.6 COMMUNICATIONS

3.6.1 Communication Channels

The management of IT based communication is in line with the patterns for other areas. There are few, if any, national standards and where these exist, they are not visible to users. As well, with few exceptions they been developed without input from users/clients. DFO uses all electronic communications channels, from mass e-mail through to Intranet, Internet and public folders. There is, however, little evidence of a clear fabric of policy indicating which system will be used for what and which communications are not appropriate for electronic distribution. The net effect of this is that every channel is used. While the management of the elements of IT that link to communication (mass e-mail, Internet, Intranet, and public folders) are all delivered with IT, they represent approaches that, if conducted on paper (letters to all staff, departmental and regional newspapers, etc.), would be managed completely within the domain of the Communications Directorate.

There is some evidence that staff are experiencing information overload. A survey conducted in 1997, during the development of the departmental Operational Greening Plan, showed that staff did not find mass e-mails, even those signed by senior staff, a valued way to obtain information. In the NCR, there were over 450 mass e-mails in 1998, ranging from job offers to a specific group and level to warnings of fire alarms on week-ends when few staff are present. An informal study conducted in Pacific Region indicated that there had been an average of 5 per day in 1998.

There is a need for compatibility, consistency and quality of information both within and among the regions and branches. The many options (Intranet, mass e-mail or public folders) make it very difficult to choose the right medium for delivery of information. Programs are at a loss to know which medium they should use to communicate. There is neither policy nor any evident source of advice that one can turn to. Public folders, what they are and how to use them, are a mystery to most departmental staff. The content of mass e-mails needs to be examined as to whether it is information that could be transmitted using another medium (such as e-mails about parking to only those who use it).

3.6.2 Web Publishing

The management of publishing information on the Intranet and Internet can be found not only in the Communications Directorate but also in program areas across the department. Web publishing has become a widespread activity since the emergence of the “hypertext” language, which permitted linking text in one document to other information resources like maps, tables, and other reports. This has been further enhanced by the development of fast “global” searching engines capable of examining millions of records for one specific piece of information. It is in fact another channel of communications, but one which is sufficiently large that it warrants special attention. This is especially true since the Internet has the potential to become an even larger expenditure. Industry Canada has implemented a small business outreach Internet activity, called “Strategis”,

which has cost over $20 million to implement with annual operating costs of several million dollars per year. PriceWaterhouseCoopers, in its publication *"Technology Forecast: 1998"*, indicated that large Internet presences routinely cost over $10 million, with electronic commerce sites (like Amazon.com, the world's largest bookstore) costing over $30 million to develop and $5 million per year to maintain because of the high costs of providing constantly changing information. While some may argue that DFO could benefit from expenditures as high as $15 million in Web publishing, no business cases were found for any of the current Web publishing activities.

This review identified that DFO spends approximately $2 million a year on Web publishing costs, including hardware, software and salary expenditures. In the survey of DFO staff, 72% of respondents indicated that they had used the internal Intranet in the previous month. The usefulness of information obtained was rated at about 4 on a scale of 5. Furthermore, 82% reported that they used the Internet at work. Some key DFO information that is for clients (such as statistical reports and fisheries regulations) is now available solely on departmental Web servers.

A very real potential exists that non-scrutinized material has been and will be mounted on Web sites, both for public consumption via the Internet and internal viewing via the Intranet. No wide-ranging controls exist to verify that the material is accurate and in stride with DFO policies and mandates. While the Communications Directorate has the responsibility for enforcing Departmental and Treasury Board standards, they indicated that they had not done any monitoring. Indeed the Pacific Region Web pages comply with neither the Departmental nor the Treasury Board "look and feel" standards.

From an efficiency point of view, no mechanism exists to ensure that Web-published material is valuable. This is a highly voluntary activity at DFO, relating more to want than need. Many groups admit to publishing on the Web "because it is fun." The majority of Web publishers do not have a clear idea who their audience is and this makes it difficult to decide what to include and what to exclude. Even when a study was done with contact groups, over 80% of the clients in the contact group had had no experience with the Internet at all. As Web publishing tools become cheaper and easier to use, it is probable that more and more material will be mounted for public viewing.

There are a couple of notable exceptions to this: a lot of Web page development in the Maritimes and Laurentian Regions has been adequately planned. Region-wide committees were struck in these Regions with an eye to defining the client and presenting more narrow, pertinent groupings of information. Such approaches represent a "best practice" and a management approach that should be more widely implemented.

3.7 TRAINING

3.7.1 Training Deficit

The management of change in the area of IT appears, from survey results, to have inadequately managed the training component. The user survey undertaken as a part of this review found that 40% of DFO employees would like training for software currently installed on their computer. The same survey indicated that approximately 2,970 people at DFO have not received training when

new software is installed and half of DFO employees (approximately 4,500 people) have not been advised of the uses or benefits of new software that has been installed. If this is addressed, a number of issues related to ease of use, reliability and reliance on the Help Desk would also be mitigated. While IM/TS staff point to the numerous courses that are offered and Intranet pages describing what courses are available, the survey results indicate that these approaches have not been effective in reaching the 50% of staff who appear to still want training.

Computer users want more training than they have received. This presumably is partially a program decision, somewhat independent of IM/TS. Training on the office suite was identified in the survey of departmental users as a need by 25% of departmental staff; however, IM/TS is offering training and commercial training is also available in every major city. The fact that program staff feel the need and have not received training on the office suite suggests that staff have not asked for training or that managers have not allocated funds to address this.

One effect of the absence of training on applications as widely implemented as the office suite is that the Help Desk function becomes burdened with simple and unnecessary requests. The Pacific Region, in moving to a Help Desk offered by internal staff rather than contractors, indicated that it was not prepared to pay a contractor $37 an hour to provide basic problem-solving in the use of Word. There are a number of other ways that this problem could be addressed. A number of management approaches are available. One approach would be to direct software-related calls to a service organization that solely does software support and may charge less than our internal costs. A second way would be to limit the number of "software operational" calls for individual users (e.g., four "office suite calls per person per year"). A third approach would be to monitor the exact nature of Help Desk calls and report this to one of the IT user/client committees for action. In some organizations there is an internal charge back system on a per call basis. This approach brings the training/help desk cost directly to individual program managers.

Clearly, the evolution of the desktop triggers a need for training. Whenever core software is changed to add new features that affect the users and require new skills or training to utilize, the costs of and arrangements for training should be established before any new versions are purchased. Given that Office 97 is still not fully implemented, consideration of the new operational demands associated with evolving the national desktop standard to Microsoft Office 2000 (currently being sold as a pre-release version to the public) should be detailed and comprehensive. This is especially true as a number of large corporations have made a needs-based decision to continue to use Office 95 (essentially the version that DFO is still using on the 486-based computers) and avoid the training, hardware and technical incompatibility issues associated with Office 97. As there was no business case analysis showing that Office 97 was required in order for DFO users to deliver their program responsibilities, the many hardware and software difficulties which accompanied this change could have been avoided.

Where specialized software (such as the Departmental Violations System, Habitat Referrals Tracking System, Abacus and others) have been rolled out, the record of staff taking training is better. It may be that managers consider office functions routine and recognize that custom applications require specialized training. Alternatively, managers of program-based systems may feel a clearer ownership of all aspects of the implementation, including training.

In the Pacific Region, there was an innovative implementation of the Office 97 desktop. A "per user" package was created and "sold" to managers for $125 per user ($100 was the cost of one half-day of training and $25 was a contribution to the cost of the software license and the accompanying CD-ROM). The full cost of the Office 97 software license was $78 per user, three times the recovered cost. Although Pacific IM/TS originally intended to offer only "complete" packages which included the training, it eventually bowed to program pressure and "sold" licenses without training to program areas at $25 per desktop. This resulted in the new software appearing on the desktops of program staff without staff having been trained in its use. The user survey results for this review confirm that program staff still wish to have this training. A business case approach, even in this case, would have allowed for better management of this IT transition.

New versions of office "desktop" software are often acquired to gain access to new features not found on older versions. It is important to assess through client-provider committees what program needs exist for these new features. Furthermore, the training necessary to use these features must be included in the consideration of costs and benefits. In the example outlined above, taking the $100 per user used by Pacific Region as a reasonable cost to the department for Office 97 training, the Office 97 license itself cost $700,000. However, it created a program need for training of $900,000 (9,000 employees at $100 each), making the actual (non hardware-related) cost $1.6 million. In all future system-wide upgrades, the costs of training must be included in the business case that supports the change. Training needs to be made a part of every change to the system and training for existing and new versions of e-mail and the desktop suite should be considered as a part of network costs.

The case has been made that often new and expensive changes, while not required by users, make the IM/TS functions easier to conduct. This does not diminish the need for a full analysis of the benefits and costs (including disruption, training and new hardware) that would accompany such a change. Certainly Microsoft is holding free seminars on Office 2000 for IT managers saying it is easier and cheaper to manage than the current Office 97, while at the same time remaining silent on the new hardware requirements and interoperability issues. As noted elsewhere in this report, a business case analysis considering products from a variety of manufacturers should precede investments of this type.

Finally, the user survey identified that between 12% and 28% of departmental staff have "given up" trying to solve a computer problem which they feel impairs their ability to perform their responsibilities. It is likely that this would be reduced if the requested training (40% of staff) were provided.

4.0 Recommendations

It is recommended that

4.1 The department move quickly to implement a decision making process that will ensure that investments in IT are fully assessed, both for their support of the program needs of the department and for their compliance with departmental standards and architecture. Such a system should clarify accountabilities for the management of all IT assets, services, standards and architecture. This process must include IM/TS staff and clients, from all

regions and the NCR. The process used to develop the Informatics Architecture document is a good model.

4.2 The department ensure that large scale IT systems are assessed using a comprehensive project assessment and planning tool. Maritimes and Laurentian Regions use a system that was developed for use in DFO and has proven helpful in ensuring the smooth implementation of large scale systems.

4.3 The department establish reliable long term funding for the IT components which are fundamental to communications and interoperability. This includes the telecommunications, hardware and software that support the WAN/LAN, as well as the standard "desktop office suite" and e-mail system. Funding for staff who operate and maintain this system (either directly or under contract) as well as the "Help Desk" and "portfolio management" staff should be included. The level of ongoing funding should recognize the rapid rate of change that is characteristic of IT, while at the same time focus on what is required for DFO to deliver its program responsibilities.

4.4 Corporate Services IM/TS conduct a Threat and Risk assessment of the network with a high priority on assessing threats from the current architecture of Internet access to DFO to determine if they represent an acceptable level of risk.

4.5 Corporate Services IM/TS in the Regions and the NCR work together to identify the products and services, including reports, acceptable response times, and levels of service that are required for the operation of the WAN. This should be used to obtain, by tender, telecommunications and network assessment and reporting services for subsequent fiscal years. Further, a complete assessment should be carried out of the products, services and levels of service that should have been provided by GTIS under the current arrangements, but were not. Should the service deficit that this analysis identifies be substantial, remedial action should be taken.

4.6 Corporate Services IM/TS take steps to notify users of the security of DFO's current electronic systems, and the degree to which they should be used for sensitive information. An assessment should be conducted to determine the extent to which DFO needs secure encryption and authentication for e-mail and financial transactions.

4.7 Corporate Services IM/TS develop, in cooperation with programs and departmental human resources staff, a mechanism to address the "training deficit" identified in this review. Over half of this "training deficit" is related to the operation of the current "desktop suite".

4.8 Corporate Services IM/TS in Regions and the NCR work with clients to establish reasonable and effective means for standardizing:

4.8.1 Acceptable levels of network performance
4.8.2 Firewall Rules
4.8.3 Levels of service to small offices, remote locations and ships
4.8.4 A mechanism for assessing the evolution of the desktop standard and e-mail

4.8.5 A suite of policy statements in the areas identified in section 3.4.1 of this report
4.8.6 What services and areas qualify for 24 hour support
4.8.7 What services and areas must have no single points of failure
4.8.8 Chargeback and support arrangements for program based large scale multi-region IT initiatives
4.8.9 IT and WAN/LAN services provided to tenant departments (e.g. NRCan)

4.9 Corporate Services IM/TS develop an effective and comprehensive needs statement for the WAN, which would include clearly stated performance criteria, reporting requirements based on the needs of IM/TS staff in NCR and the Regions, and penalties for failure to perform according to specified standards and use this as the basis for contracting for the WAN services so as to avoid the many weaknesses identified in the current arrangements.

4.10 Steps taken by regional Corporate Services IM/TS staff to work towards addressing architecture and firewall inconsistencies be expanded to include NCR staff and clients so that a comprehensive solution that recognizes client needs can be implemented.

4.11 Corporate Services IM/TS and the Communications Directorate work together to identify an orderly and reasonable approach to the use of electronic communications and information sharing. Consultations should include program areas that currently sponsor Web publishing both internally and on the open Internet.

4.12 The Coast Guard, in cooperation with GTIS and Corporate Services IM/TS, assess the degree to which program needs can be met and savings can be achieved through harmonized acquisition of telecommunications services. Such an assessment is especially desirable given the technical similarities of the soon to be implemented INNAV system to the equipment and links currently operated by Corporate Services IM/TS.

4.13 Corporate Services IM/TS advance the Acceptable Use Policy for IT resources so as to provide clarity on what is, and what is not acceptable for DFO employees. (Policy was issued May 28, 1999).

ACKNOWLEDGEMENTS AND THANKS

Special thanks are due to the staff of Corporate Services IM/TS in the NCR and in all regions. A special vote of thanks is due to the Director General, IM/TS, who throughout the exercise worked hard to ensure that the review team had the information that it required. In addition, several IM/TS Directors and many staff from the technical and support side of the informatics function have taken time to make helpful observations, review draft findings and explain the intricacies of a complex system.

5.0. MANAGEMENT ACTION PLAN

The Context of The Review

Fisheries and Oceans has a complex array of missions reliant on information technology for a number of key aspects. This reliance, coupled with the geographic scope of the department, has resulted in early and continuing investment in information technology.

Science, as an activity, has used computers since they first became available. Certainly some of the pivotal and ground breaking uses of computers to compile and analyze large volumes of information were done by DFO Science staff. Further the scientific community was the foundation on which the Internet was based. DFO Science staff use the Internet for communication and collaboration with scientists around the world and have done so since this first became possible. Similarly the distribution of information to clients and to the academic community is heavily reliant on information technology.

The Coast Guard, because of their responsibilities for navigation and search and rescue has also been on the forefront information technology. Information flows related to navigation and safety come from all parts of Canada, from remote light stations to busy harbours.

DFO as a department has also been an early adopter of communications, analysis and delivery mechanisms that are based on information technology. The implementation of a national electronic systems for mail, financial and human resource systems is evidence of this. The survey conducted as a part of this review found that virtually all respondents (97.4%) reported that they had access to or used a computer in their regular work activities. Department-wide access to computers appears to be consistent, as at least 90% of respondents in all regions and sectors indicated that they use a computer in their regular work activities.

DFO has made, and continues to make major investments in information technology. During the period of the review DFO was spending $6,650 per employee per year on information technology. This review has identified and made recommendations on important areas for action. When the recommendations found in this report have been implemented, a better and more cost effective use of information technology will result.

5.0. MANAGEMENT ACTION PLAN

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
1. The department move quickly to implement a decision making process that will ensure that investments in IT are fully assessed, both for their support of the program needs of the department and for their compliance with departmental standards and architecture. Such a system should clarify accountabilities for the management of all IT assets, services, standards and architecture. This process must include IM/TS staff and clients, from all regions and the NCR. The process used to develop the Informatics Architecture document is a good model.	The ISC has now been established and has recommended a departmental informatics project proposal review process. This will provide for a corporate review of project proposals with a view to reducing risks, assessing conditions for success, reducing duplication, and leveraging the results in support of the strategic directions and business priorities of the DFO. Our strategy is to implement the approval process for larger scale system initiatives, to prove it right and valuable, and then to implement similar processes (at other levels and perhaps on a smaller scale) for smaller initiatives. In the meantime, the model is being assessed for use within several regions and sectors.	Director, Planning and Information Management Services Branch	September 1, 2000
2. The department ensure that large scale IT systems are assessed using a	For large scale IT projects, Application Services Branch (ASB) will promote the use of two key Project Management skillsets *Software Project Planning* and *Software Project Tracking and*	Director, Application Services Branch	ASB training & seminars have started. June 2000 at the latest

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
comprehensive project assessment and planning tool. Maritimes and Laurentian Regions use a system that was developed for use in DFO and has proven helpful in ensuring the smooth implementation of large scale systems.	*Oversight*. These Project Management processes are an integral part of the Treasury Board Enhanced Management Framework (EMF). They will be promoted by ASB through seminars in NCR and in the regions using the EMF as the framework. ASB staff members are currently being trained on both and are being encouraged to pursue Project Management Certification. Project Management tools are also being evaluated. We will propose a standard tool kit for project management to DMC/DEC.		for tool kit recommendation.
3. The department establish reliable long term funding for the IT components which are fundamental to communications and interoperability. This includes the telecommunications, hardware and software that support the WAN/LAN, as well as the standard "desktop office suite" and e-mail system. Funding for staff who operate and maintain this system (either directly or under contract) as well as the "Help	➢ Submit option analysis and recommendation to ISC/DMC for decision regarding the on-going A-Base funding requirements for the DFO Shared Informatics Infrastructure addressing consistent and reasonable service levels throughout the Department. ➢ Submit the Shared Informatics Infrastructure capital refreshment requirements included in the LTCP to DMC for funding approval.	DG, IM&TS Director, Planning and Information Management Services	January 2000 -- A-Base has been revised, and we are developing a DFO-wide cost-recovery strategy for informatics. Target: June 2000 Fall 99 -- requirements have been submitted. LTCP not yet finalized & approved. Fall 99 -- all

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
Desk" and "portfolio management" staff should be included. The level of ongoing funding should recognize the rapid rate of change that is characteristic of IT, while at the same time focus on what is required for DFO to deliver its program responsibilities.	➢ Ensure that national and regional IM&TS organizations participate fully in the DFO Business Planning process, and LTCP asset identification, refreshment, investment and planning process.	Director, Planning and Information Management Services	have participated
4. Corporate Services IM/TS conduct a Threat and Risk assessment of the network with a high priority on assessing threats from the current architecture of Internet access to DFO to determine if they represent an acceptable level of risk.	Corporate Services IM/TS will conduct a full threat and risk assessment of the national infrastructure including the location and policy structure on all firewalls and the architecture of the electronic mail system by September 1, 2000	Director, Technology Services	September 1, 2000
5. Corporate Services IM/TS in the Regions and the NCR work together to identify the products and services, including reports, acceptable	Corporate Services IM/TS in the Regional and NCR will work to identify the products and services including reports, acceptable response times and levels of service that are required for the operation of the WAN.	Director, Technology Services	September 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
response times, and levels of service that are required for the operation of the WAN. This should be used to obtain, by tender, telecommunications and network assessment and reporting services for subsequent fiscal years. Further, a complete assessment should be carried out of the products, services and levels of service that should have been provided by GTIS under the current arrangements, but were not. Should the service deficit that this analysis identifies be substantial, remedial action should be taken.			
6. Corporate Services IM/TS take steps to notify users of the security of DFO's current electronic systems, and the degree to which they should be used for sensitive information.	Corporate Services IM/TS will send a reminder to all users of the email system every quarter reminding them that this system should not be used for secure or sensitive transmissions.	Director, Technology Services	September 1, 2000 and ongoing

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
An assessment should be conducted to determine the extent to which DFO needs secure encryption and authentication for e-mail and financial transactions.			
7. Corporate Services IM/TS develop, in cooperation with programs and departmental human resources staff, a mechanism to address the "training deficit" identified in this review. Over half of this "training deficit" is related to the operation of the current "desktop suite".	Regional user committees will be used to scope the "end user" training deficit and develop cost estimates and an action plan in conjunction with IM&TS and HR representatives. Corporate Services is moving into a "learning organization" mode, and we will ensure that our partners are in on it and will present recommendations to DMC.	Regional Directors of Informatics (all regions)	Draft action plan for March 31, 2000 March 31, 2000
8. Corporate Services IM&TS in Regions and the NCR work with clients to establish reasonable and effective means for standardizing: 1) Acceptable levels of network	Corporate Services IM/TS will develop a workplan to address each issue and table a point by point action plan for each of these at the National Informatics Committee by September 1, 2000	Director, Technology Services	September 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
performance 2) Firewall Rules 3) Levels of service to small offices, remote locations and ships 4) A mechanism for assessing the evolution of the desktop standard and e-mail 5) A suite of policy statements in the areas identified in section 3.4.1 of this report 6) What services and areas qualify for 24 hour support 7) What services and areas must have no single points of failure 8) Chargeback and support arrangements for program based large scale multi-region IT initiatives 9) IT and WAN/LAN services provided to tenant departments (e.g. NRCan)			
9) Corporate Services IM/TS develop an effective and comprehensive needs statement for the WAN, which would include clearly stated performance criteria, reporting requirements based	Telecommunications services will be acquired to meet specified performance and security targets.	Director, Technology Services	Commence April 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
on the needs of IM/TS staff in NCR and the Regions, and penalties for failure to perform according to specified standards and use this as the basis for contracting for the WAN services so as to avoid the many weaknesses identified in the current arrangements.			
10) Steps taken by regional Corporate Services IM/TS staff to work towards addressing architecture and firewall inconsistencies be expanded to include NCR staff and clients so that a comprehensive solution that recognizes client needs can be implemented.	Implement and refine current firewall replacement and management plan, working with clients, as part of our on-going management and maintenance of the infrastructure.	Director, Technology Services	September 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
11) Corporate Services IM/TS and the Communications Directorate work together to identify an orderly and reasonable approach to the use of electronic communications and information sharing. Consultations should include program areas that currently sponsor Web publishing both internally and on the open Internet.	Corporate Services IM/TS will work with DFO Communications to develop a comprehensive plan that will consolidate DFO's WEB presence and ensure that systematic and standardized approaches are established, and that outdated and irrelevant materials are removed.	Director, Planning and Information Management Services / Director Operations Branch, Communications	April 1, 2000
12) The Coast Guard, in cooperation with GTIS and Corporate Services IM/TS, assess the degree to which program needs can be met and savings can be achieved through harmonized acquisition of telecommunications services. Such an assessment is especially	Corporate Services IM/TS will meet with staff from the Coast Guard to identify where harmonized acquisition of telecommunications services would be beneficial. A report on theses discussions will be provided to the National Informatics Committee by September 1, 2000	Director, Technology Services / DG, Technical and Operational Services - CCG	April 1, 2000

RECOMMENDATIONS	MANAGEMENT ACTION PLAN	OFFICER OF PRIME INTEREST	INITIAL TARGET DATE
desirable given the technical similarities of the soon to be implemented INNAV system to the equipment and links currently operated by Corporate Services IM/TS.			
13) Corporate Services IM/TS advance the Acceptable Use Policy for IT resources so as to provide clarity on what is, and what is not acceptable for DFO employees.	Corporate Services IM/TS will routinely monitor Internet use, as called for in Treasury Board Secretariat policy, and report the findings to the National Informatics Committee quarterly. Further, IM/TS will ensure that action is taken when any unacceptable uses are identified.	Director, Planning & Information Management Services	Completion date: May 31, 2000