Internal Audit Bureau
Bureau de vérification interne

Human Resources Development Canada — **Développement des ressources humaines Canada**
Internal Audit Bureau — **Bureau de vérification interne**

NATIONAL REPORT

Assessment of Information Technology Security

Project No.: 442/98

Project Team

Director General:	*J.K. Martin*
Audit Director:	*J.R. Clark*
Team Leaders:	*P. LePage*
	F. Gloade
Auditors:	*K. Jevons*
	M. Winterburn
Consultants:	*Progestic International Inc.*

APPROVAL: **Original copy signed by:**

DIRECTOR: *J.R. Clark* *September 30, 1999*
Date

DIRECTOR GENERAL: *James K. Martin* *September 30, 1999*
Date

September 1999

TABLE OF CONTENTS

APPENDICES

1.0 EXECUTIVE SUMMARY

During March and April, 1999, the Internal Audit Bureau (IAB) visited selected national, regional and local sites in conducting HRDC's Assessment of Information Technology (IT) Security. The IAB conducted this assessment within the context of the Federal Government's IT Governance Framework (refer to Appendix A) and HRDC's IT security standards.

Based upon the IAB's research of other similar federal and private organizations, HRDC's IT Security is satisfactory. HRDC is progressing toward a more comprehensive approach to IT security as evidenced from it's recent (May 1999) vision/strategy which addressed IT security. The delivery and support of IT security is organizationally dispersed amongst many people who have varying procedures, resulting in uncertainty as to roles, responsibilities, accountabilities, authorities and reporting relationships. Since few people know of the existence of the IT security policies and procedures, personnel knowledge of IT security standards and practices needs improvement.

Findings

- Since the creation of HRDC, programs and corporate services have maintained their own, separate processes when dealing with IT security. While HRDC Systems is the department's functional IT security group, these unique processes contribute to having too many people with different procedures involved in HRDC's IT security management.

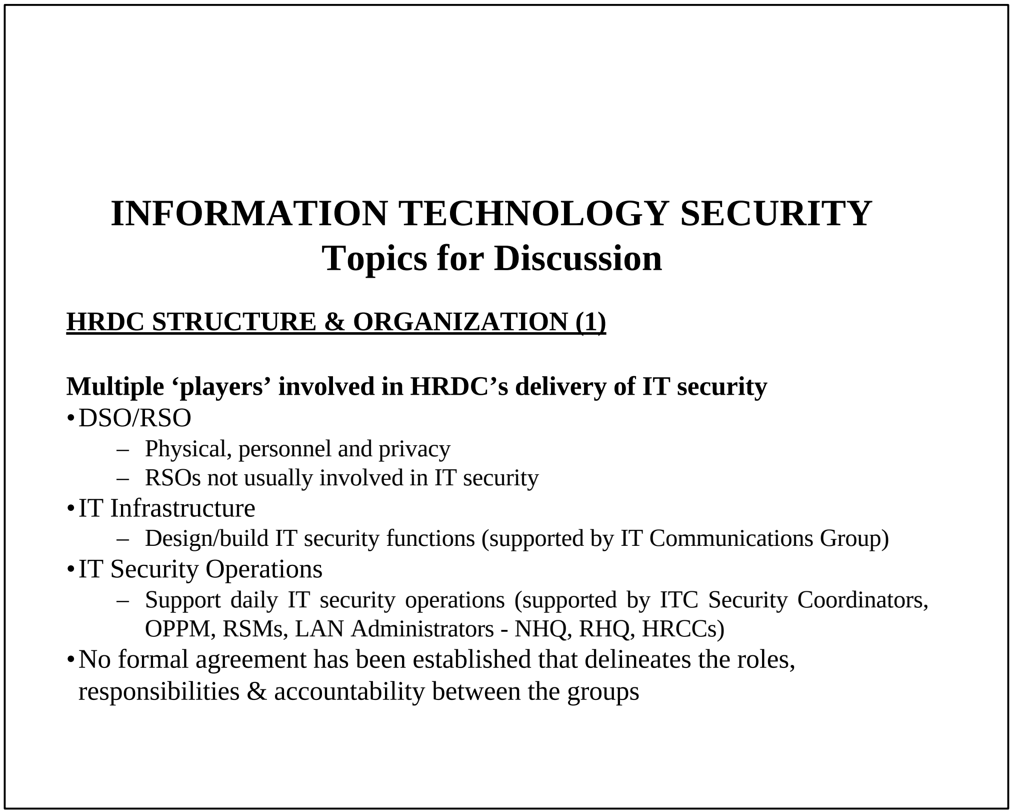
- Since the ITCs now report to NHQ Systems, regions believe they no longer have a 'Regional IT Security Officer', a role traditionally undertaken by ITC staff. As a result, regions no longer have line authority for managing regional IT security. This has left both a functional and operational void in the regions.

- Many people involved with IT security are not aware of HRDC's IT security policies and procedures, even though 'IT Security' is part of HRDC's Systems web site. Additionally, hard copies of IT security-related documents are regularly distributed to HRDC personnel, however, their knowledge level of IT security policies and procedures is not good. For example, user IDs/passwords for accessing HRDC systems are not regularly monitored contributing to people with duplicate or inappropriate user codes.

- Security awareness/orientation sessions for HRDC personnel rarely include IT security.

Next Steps

- HRDC management implements the recommendations offered in this report, with particular attention to streamlining the organizational structure and processes to manage IT security at all levels, and enhancing the knowledge and awareness of all HRDC personnel regarding IT security.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

HRDC STRUCTURE & ORGANIZATION (1)

Multiple 'players' involved in HRDC's delivery of IT security

- DSO/RSO
  - Physical, personnel and privacy
  - RSOs not usually involved in IT security
- IT Infrastructure
  - Design/build IT security functions (supported by IT Communications Group)
- IT Security Operations
  - Support daily IT security operations (supported by ITC Security Coordinators, OPPM, RSMs, LAN Administrators - NHQ, RHQ, HRCCs)
- No formal agreement has been established that delineates the roles, responsibilities & accountability between the groups

NOTE: The chart on page 6 depicts HRDC's current organizational IT Security structure

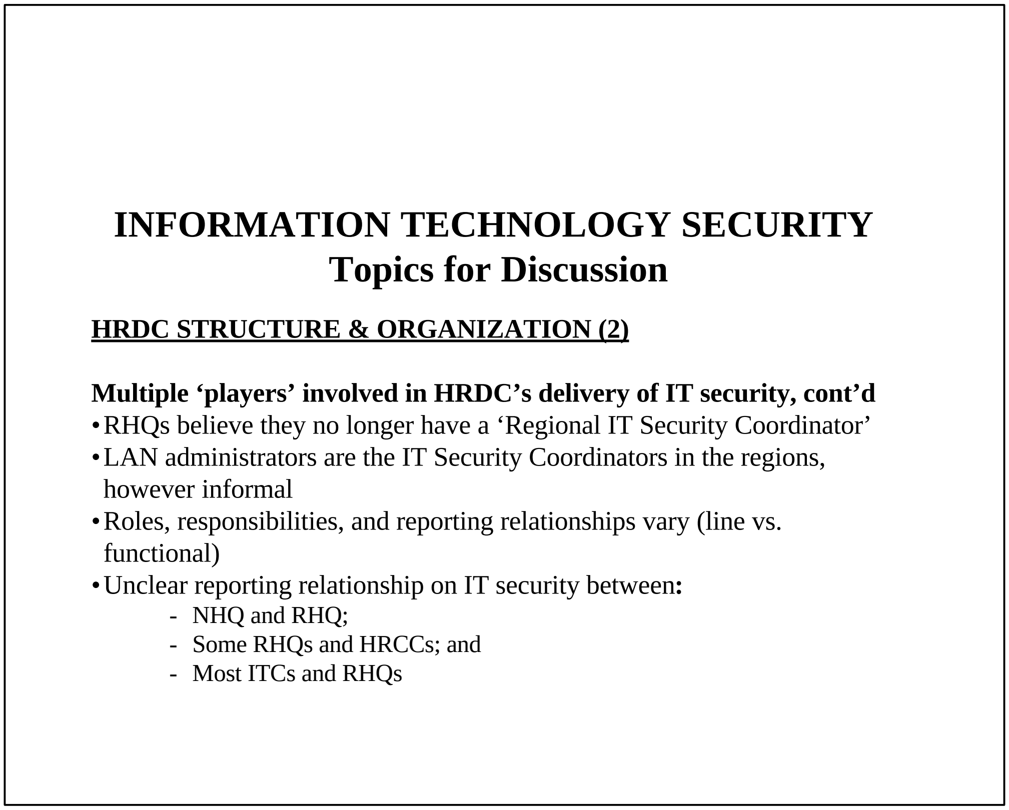
DSO - A formal Departmental Security Officer (DSO) position is established and reports to the ADM, Finance & Administrative Services (FAS). The DSO is responsible for Privacy, Physical and Personnel security.

RSOs - Most Regional Security Officers (RSOs) felt they had very little to do with IT security. Physical and personnel security were identified as their main areas of responsibilities (refer to further comments on next slide).

NHQ IT Security Infrastructure - An NHQ IT Security function reports to the DG, Infrastructure within HRDC's Systems' and provides front-end design and building of IT security tools along with functional direction to the regions and ITCs. Within Infrastructure, IT Communications (telecommunications) works with the IT Security function in developing and revising IT security tools related to the infrastructure (e.g. firewalls).

IT Security Operations- The IT Security Operations reports to the DG, Operations within HRDC's Systems. Its role is to concentrate on daily IT security operations, user awareness, back-end maintenance/support, and also provides functional direction to the regions and ITCs. Staffing is underway to support this process.

Conclusion- A formal agreement has not been established that delineate the respective roles, responsibilities and accountabilities between the three organizations. Currently this processes is done, however informal.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

HRDC STRUCTURE & ORGANIZATION (2)

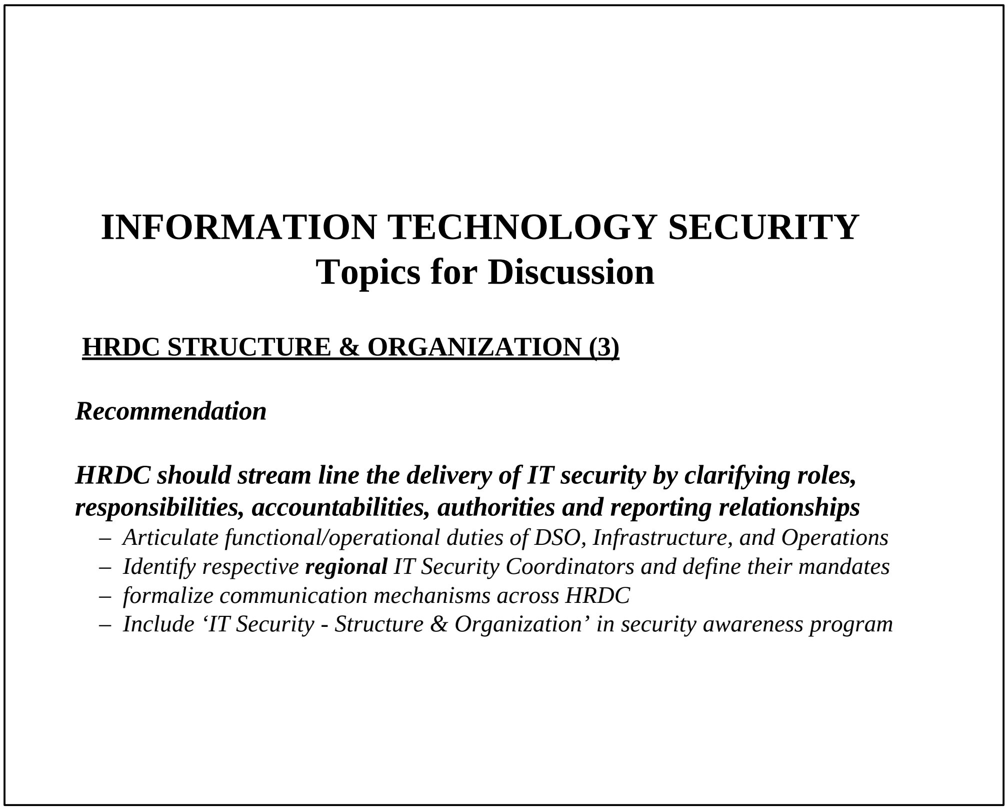
Multiple 'players' involved in HRDC's delivery of IT security, cont'd

- RHQs believe they no longer have a 'Regional IT Security Coordinator'
- LAN administrators are the IT Security Coordinators in the regions, however informal
- Roles, responsibilities, and reporting relationships vary (line vs. functional)
- Unclear reporting relationship on IT security between**:**
  - NHQ and RHQ;
  - Some RHQs and HRCCs; and
  - Most ITCs and RHQs

Regional IT Security Coordinator - All regions' Security Policy and Procedures Manual identify a "Regional IT Security Coordinator" and related duties. It is unclear if such a role still exists since the ITCs now report to NHQ. All four regions visited believed that they no longer have a Regional IT Security Coordinator as part of their formal regional organization. The RHQs, to which the ITCs used to report, still maintain an informal relationship with the ITC Security Coordinator.

Variances at the regional level - All Regional Systems Managers (RSMs) felt they had functional authority for their regional and local LAN Administrators, however, some did not believe this included IT security. The latter felt that IT security was primarily the responsibility of either Infrastructure and/or Operations at NHQ.

LAN Administrators - At the HRCCs visited, LAN Administrators were identified as the primary IT security resource. In all regions, the RSM has functional authority for LAN Administrators and in some regions also has line authority. For those with functional authority only, the HRCC Directors have line authority for their LAN administrators.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

<u>HRDC STRUCTURE & ORGANIZATION (3)</u>

Recommendation

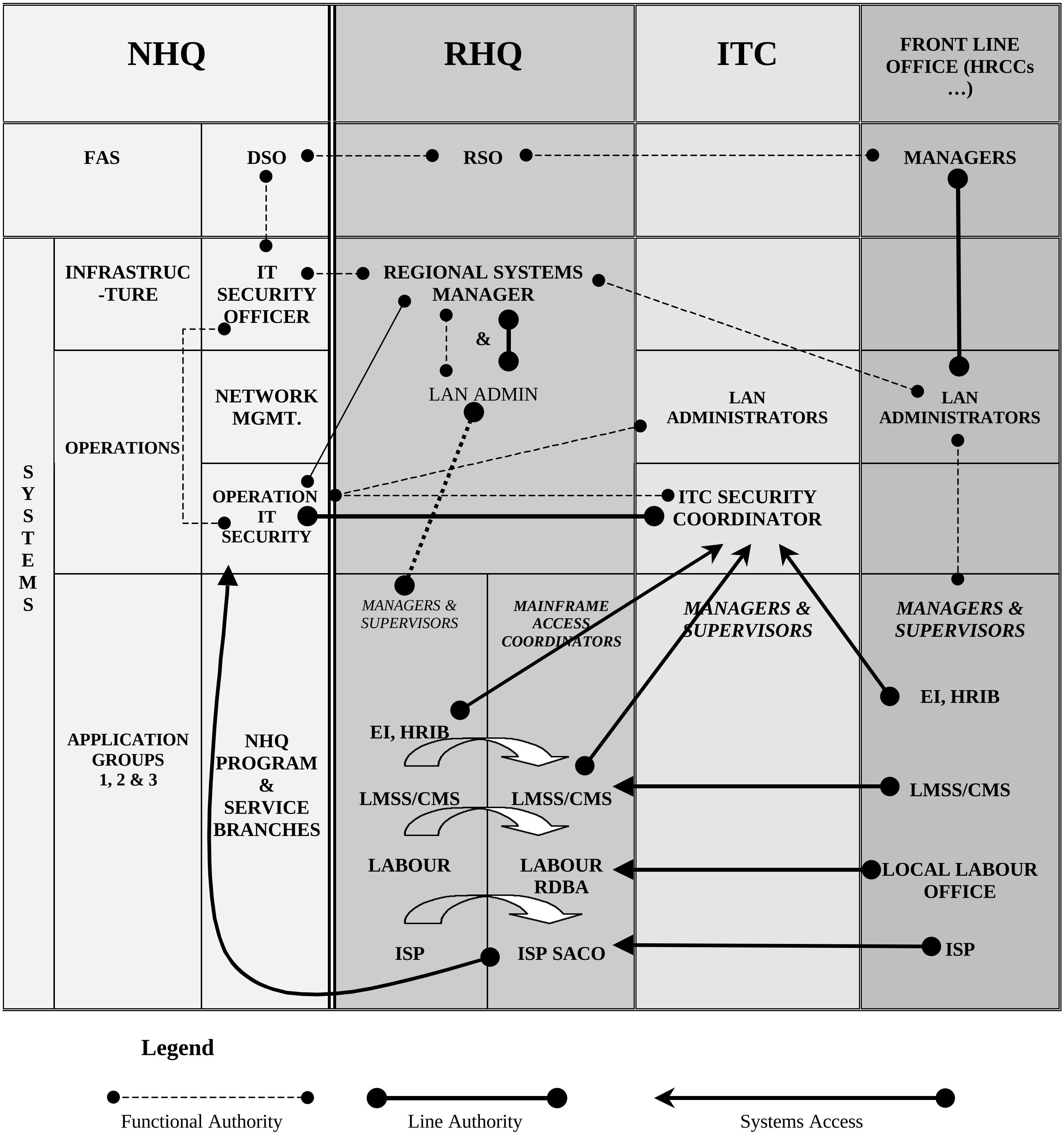
HRDC should stream line the delivery of IT security by clarifying roles, responsibilities, accountabilities, authorities and reporting relationships

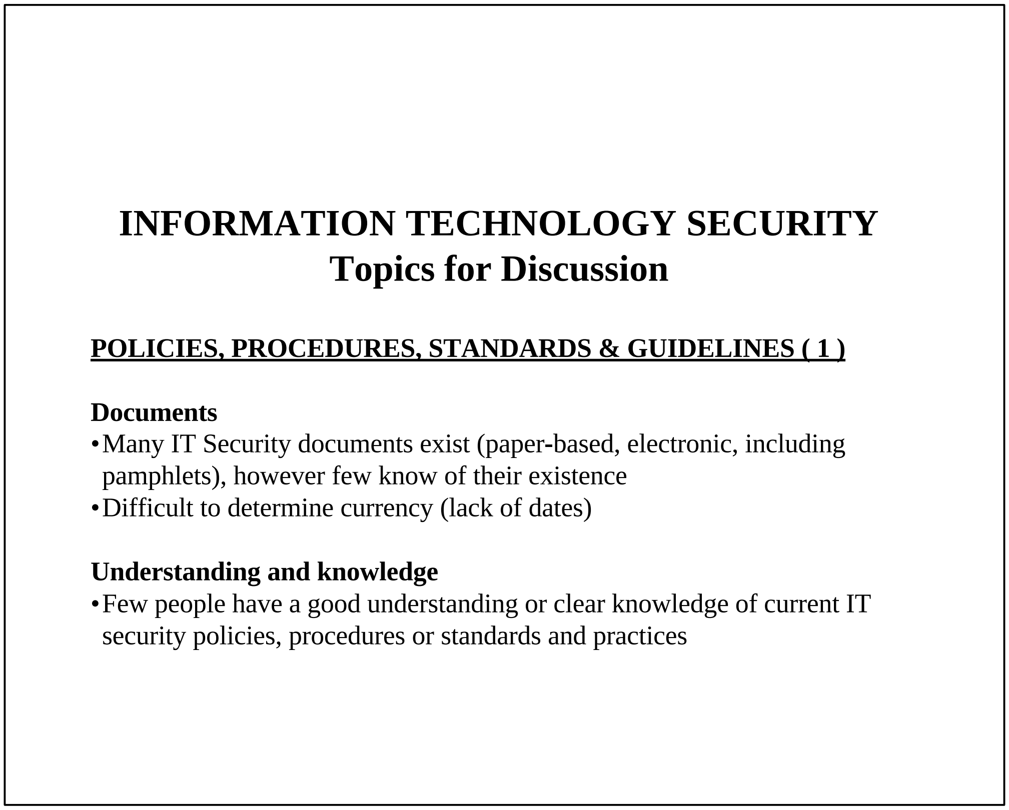
- *Articulate functional/operational duties of DSO, Infrastructure, and Operations*
- *Identify respective* ***regional*** *IT Security Coordinators and define their mandates*
- *formalize communication mechanisms across HRDC*
- *Include 'IT Security - Structure & Organization' in security awareness program*

Conclusion

Due to the dispersion of how IT security is delivered throughout HRDC, the IAB concluded that most people interviewed had difficulty accurately indicating how the organizational structure worked and who was accountable for what aspects of IT security within HRDC. This confusion of "who was responsible/accountable for what" is even more pronounced at the regional and local levels. This fragmentation has also caused some groups to not always know what other groups, which are involved in IT security, are doing or producing.

In the absence of strong regional IT security leadership, and a stronger functional direction from NHQ, the delivery of IT security is at the operational level. As a result, the quality of IT security at the sites visited was more dependant upon the individuals' IT security awareness, training, background and experience, rather than clearly defined, roles, responsibilities and accountability or functional guidelines.


NHQ
RHQ
ITC
FRONT LINE OFFICE (HRCCs …)
FAS
DSO
RSO
MANAGERS
SYSTEMS
INFRASTRUC-TURE
IT SECURITY OFFICER
REGIONAL SYSTEMS MANAGER
&
LAN ADMIN
OPERATIONS
NETWORK MGMT.
LAN ADMINISTRATORS
LAN ADMINISTRATORS
OPERATION IT SECURITY
ITC SECURITY COORDINATOR
APPLICATION GROUPS 1, 2 & 3
NHQ PROGRAM & SERVICE BRANCHES
MANAGERS & SUPERVISORS
MAINFRAME ACCESS COORDINATORS
MANAGERS & SUPERVISORS
MANAGERS & SUPERVISORS
EI, HRIB
EI, HRIB
LMSS/CMS
LMSS/CMS
LMSS/CMS
LABOUR
LABOUR RDBA
LOCAL LABOUR OFFICE
ISP
ISP SACO
ISP
Legend
Functional Authority
Line Authority
Systems Access



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

POLICIES, PROCEDURES, STANDARDS & GUIDELINES (1)

Documents

- Many IT Security documents exist (paper-based, electronic, including pamphlets), however few know of their existence
- Difficult to determine currency (lack of dates)

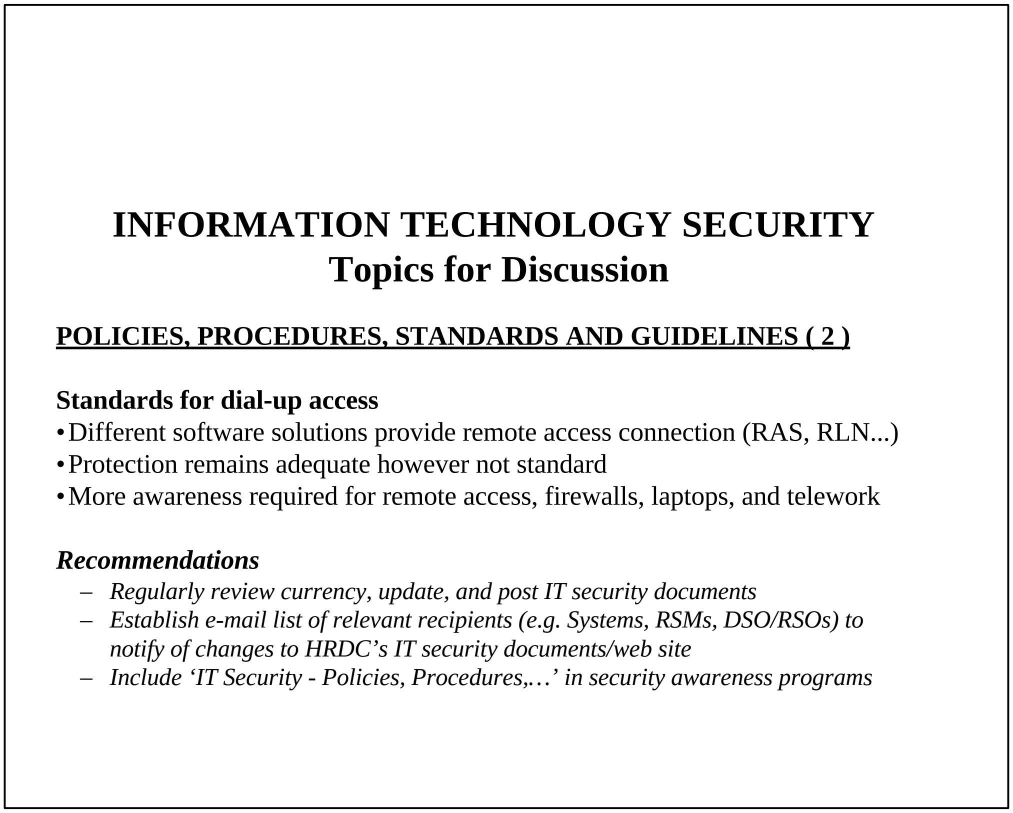
Understanding and knowledge

- Few people have a good understanding or clear knowledge of current IT security policies, procedures or standards and practices

Where are they located on the Intranet? – Despite various efforts by HRDC to promulgate IT security, few users (NHQ, RHQ, HRCCs and ITCs) reported knowing of the electronic sites where current HRDC IT security policies, standards and procedures reside. Since this assessment commenced, a ‘pop-up’ menu now appears during initial log-in to for all desktop computers, advising users of appropriate intranet usage. Also, the IT Security intranet site has been updated to include an appropriate index and additional documentation. HRDC users should be notified of these updates to the web-site.

Few people know what exists - Most HRDC personnel do not have a good understanding or clear knowledge of current IT security policies, guidelines, procedures and standards despite HRDC’s IT Security intranet site. Consequently, the IAB believes that this lack of awareness for current IT security policies and procedures contributes to the variation in IT security practices between NHQ, regions, ITCs and HRCCs (as mentioned in previous slide).

Inconsistent security measures - The regional perception that they lack a regional IT Security Coordinator has left RHQs and local offices relatively on their own for the delivery of operational IT security measures. This perception, mixed with the variances among RHQ/ HRCCs LAN Administrators’ knowledge, expertise, and concerns for IT security measures, has led to inconsistent IT security measures, such as various IT security risks not being appropriately addressed (e.g. cancellation of redundant user codes/passwords), and some regions independently developing their own security awareness program including an IT component. Likewise, we noticed that IT security measures associated to the HRCCs are frequently left to the discretion of the LAN administrators. Since most LAN Administrators received no formal IT security training or had little background in IT security, their concerns and expertise for IT security varied and led to inconsistent practices at the local level.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

<u>POLICIES, PROCEDURES, STANDARDS AND GUIDELINES (2)</u>

Standards for dial-up access

- Different software solutions provide remote access connection (RAS, RLN...)
- Protection remains adequate however not standard
- More awareness required for remote access, firewalls, laptops, and telework

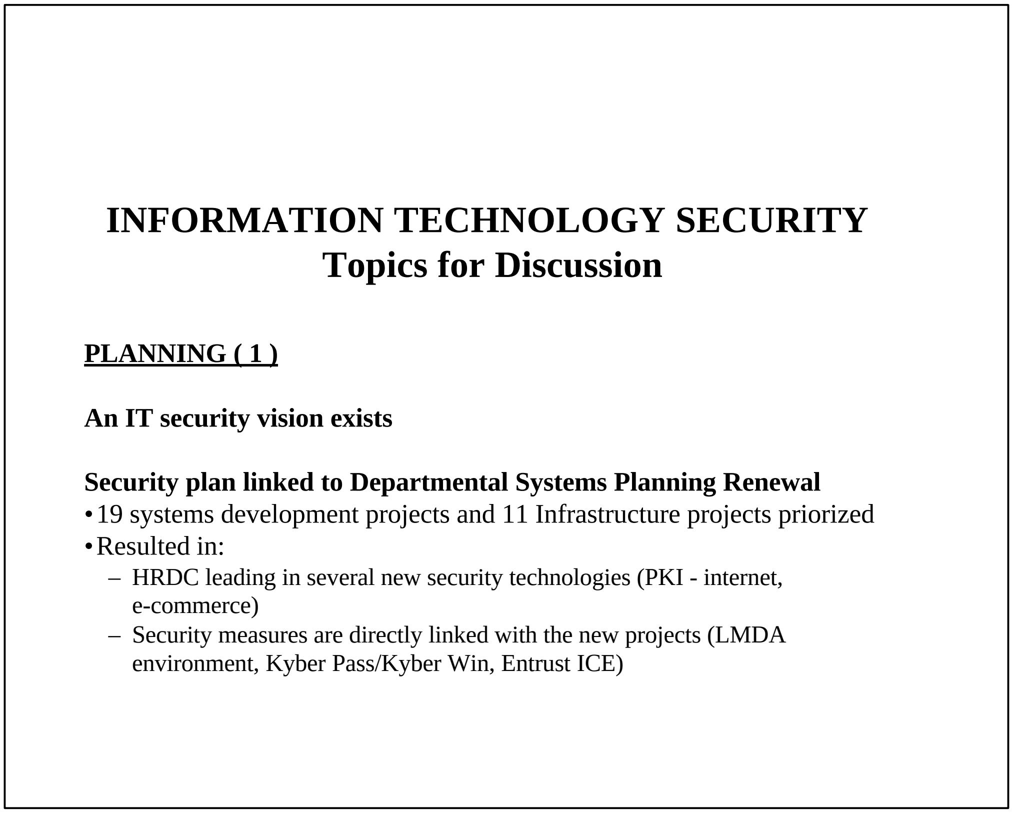
Recommendations

- *Regularly review currency, update, and post IT security documents*
- *Establish e-mail list of relevant recipients (e.g. Systems, RSMs, DSO/RSOs) to notify of changes to HRDC's IT security documents/web site*
- *Include 'IT Security - Policies, Procedures,…' in security awareness programs*

Different remote access security software exist - The review identified that different remote access security software are used across HRDC such as ReachOut, Remote Access Software, Remote Link Network, and Racal Guard Data Watchword. Interviewees mentioned several rationales for the implementation of these software such as better security, ease of use, and faster connection time. Awareness of remote access standards needs to be reinforced.

Requirements for documents - Several interviewees identified the need to have a more detailed policies for laptops and telework, procedures to support the firewall policy, standards for remote access (dial-up) and guidelines to build LAN rooms and selecting off-site storage locations.

Note: When generating an action plan the above recommendations should consider the Structure and Organization recommendations of this report.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

PLANNING (1)

An IT security vision exists

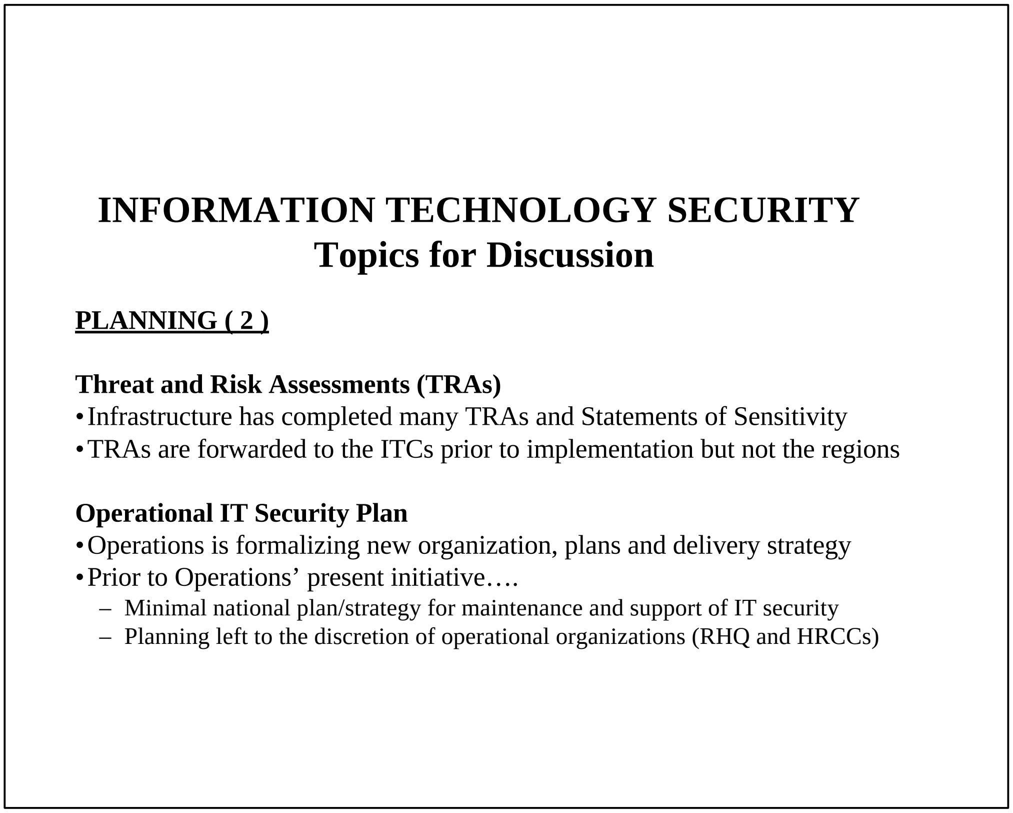
Security plan linked to Departmental Systems Planning Renewal

- 19 systems development projects and 11 Infrastructure projects priorized
- Resulted in:
  - HRDC leading in several new security technologies (PKI - internet, e-commerce)
  - Security measures are directly linked with the new projects (LMDA environment, Kyber Pass/Kyber Win, Entrust ICE)

IT security vision - In its 1998/99 ‘Compliance with the Management Board Decision on Systems, July, 1995’ and ‘ITC Cross-Sectional Review’, the IAB noted that ‘an integrated vision, plan and strategy do not exist (specific to IT security)’. Since then, an IT security vision/strategy has been produced by Infrastructure, integrating such items as:

- single user-ID and logon procedure for staff, with access control to application and services transparent to the end user;
- the ability to handle Internet based transactions processed in a secured fashion;
- secure data exchange including e-commerce with partners; and
- a security mechanism consistent with financial institutions for interaction with the Canadian public.

Link with new projects to create an IT plan - HRDC’s IT security planning is directly related to the specific IT projects which have been priorized from the Departmental Systems Planning Renewal (DSPR) process. It was reported to the IAB that for 1999/00, HRDC priorized 19 systems development and 11 infrastructure projects from the DSPR process. As the Project Review Committee assesses these projects, appropriate IT security plans/decisions are incorporated. These security measures are directly linked with new projects such as access to HRDC data in a LMDA environment, Kyber Pass/Kyber Win, Entrust ICE and remote access software.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

PLANNING (2)

Threat and Risk Assessments (TRAs)

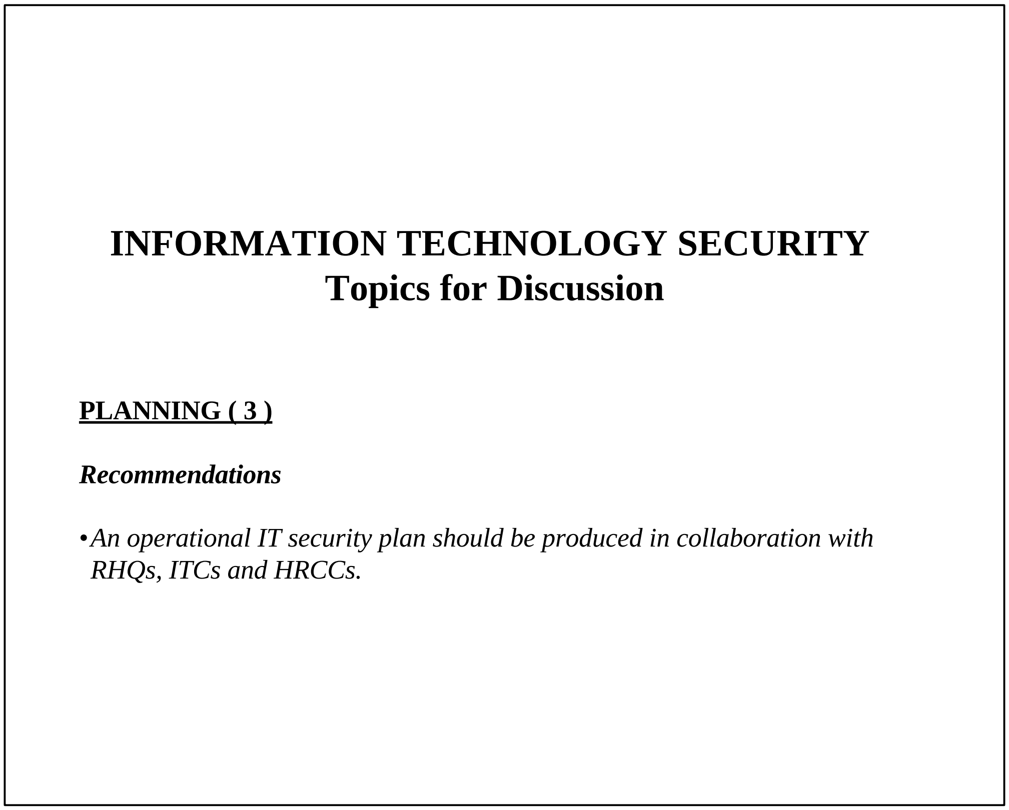
- Infrastructure has completed many TRAs and Statements of Sensitivity
- TRAs are forwarded to the ITCs prior to implementation but not the regions

Operational IT Security Plan

- Operations is formalizing new organization, plans and delivery strategy
- Prior to Operations' present initiative….
  - Minimal national plan/strategy for maintenance and support of IT security
  - Planning left to the discretion of operational organizations (RHQ and HRCCs)

TRAs completed by Infrastructure - At NHQ, Threat and Risk Assessments (TRAs) are mainly completed for projects that are supported by the Project Review Committee. During the 1998/99 fiscal year, the Infrastructure's IT Security group completed approximately 25 TRAs identifying weaknesses, potential vulnerabilities, as well as recommendations to improve the situation and decrease risks. Most TRAs were completed as a proactive measure prior to the development or implementation of application systems or operational infrastructure changes. Regions and HRCCs showed interest in receiving the results of the TRAs' since they believed the information to be useful during the field implementation process. One example given to support this request was the recent implementation of the laptops for the EI Overpayment agents. Regions tried to identify the best security measures prior to deploying these laptops since they will contain sensitive data and use remote access to link with corporate applications. Regions mentioned that implementation guidelines were not provided and, as a result, they had to determine their own pre-implementation security measures. NHQ is continuing to work on the remote connectivity issue (e.g. LOIS, Investigation & Control).

Operations IT Security Plan - In addition to the Infrastructure Branch, Systems' Operations Branch has a role in delivering IT security. The IT Security Operations group is now staffing their new IT security organization to address network, platform and EasyLock security components. The IAB understands that once the Operations group is properly staffed, an operational security plan will be formalized.



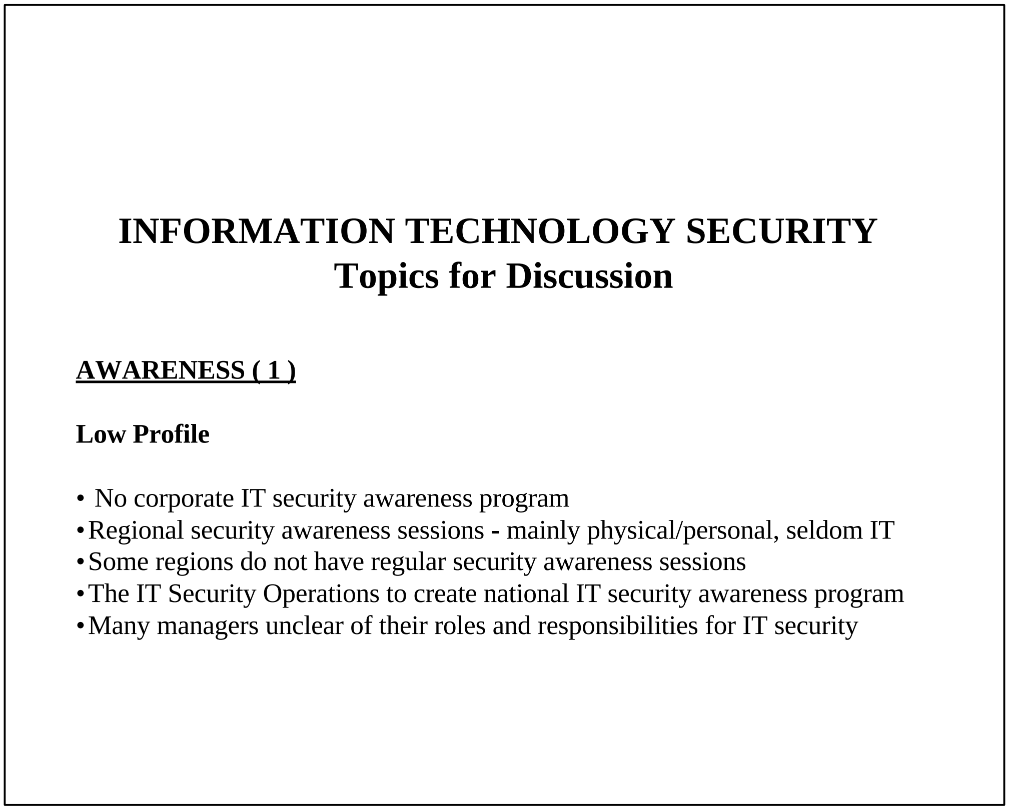
INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

PLANNING (3)

Recommendations

- *An operational IT security plan should be produced in collaboration with RHQs, ITCs and HRCCs.*

Note: When generating an action plan the above recommendations should consider the Structure and Organization recommendations of this report.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

<u>**AWARENESS (1)**</u>

Low Profile

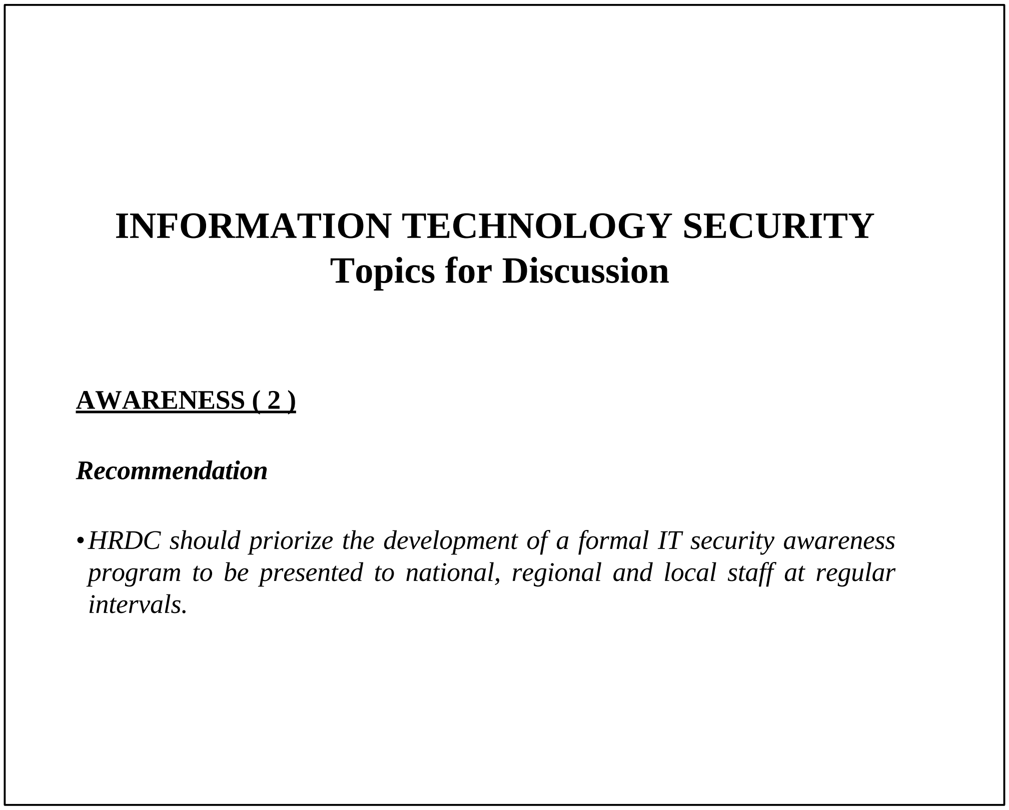
- No corporate IT security awareness program
- Regional security awareness sessions **-** mainly physical/personal, seldom IT
- Some regions do not have regular security awareness sessions
- The IT Security Operations to create national IT security awareness program
- Many managers unclear of their roles and responsibilities for IT security

No formal corporate IT security awareness program - Currently, a formal national IT Security Awareness program has not been established within HRDC. Historically, the Departmental and Regional Security Officers have been responsible for physical and personnel security; NHQ Systems has been responsible for IT security. New staff are not always informed of their IT security responsibilities and accountability nor exposed to departmental IT security rules and regulations due to the absence of IT security awareness sessions.

IT security awareness initiatives - The IAB noted that some initiatives were undertaken to enhance IT security awareness and were well received.

- Attendees at the NHQ's recent Security Symposium told the IAB that IT security awareness was part of the agenda. Since this symposium was designed for NHQ Systems (Operations/ ITCs), there was no regional participation.
- During the Ontario region's "LAN Tech 99 Conference", a NHQ Operations spokesperson was invited to specifically address IT security.
- One RSO has taken the initiative to have an ITC's Security Coordinator attend regional/local office security awareness sessions to specifically address IT security.
- The IAB also noted that the New Brunswick region has a close working relationship with the RCMP, which help them in dealing with IT security incidents.
- HRDC has contracted the RCMP to conduct IT Security LAN Administration workshops.

Security responsibilities of staff and managers - The IAB noticed that IT security does not have a high profile and is not entrenched in HRDC's culture. While most managers and staff are appreciative of IT Security, there is a need to ensure that they clearly understand their role, responsibilities and accountability in that matter.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

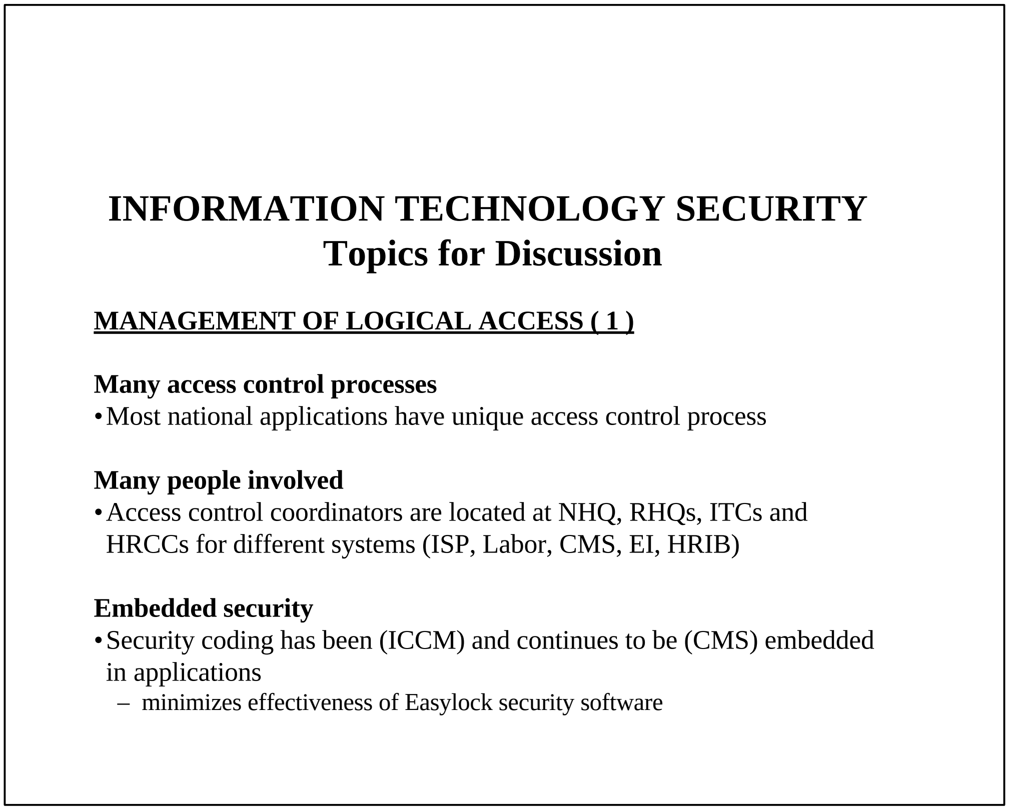
AWARENESS (2)

Recommendation

- *HRDC should priorize the development of a formal IT security awareness program to be presented to national, regional and local staff at regular intervals.*

Lack of awareness for IT security responsibility and accountability - HRCC Directors and HRCC Managers were aware of their security responsibilities relating to protecting their physical premises, assets and the personal security of staff and clients. However, IT security was primarily viewed as a technical issue which either the LAN Administrator or some person/group managed at either RHQ and/or NHQ. Likewise, staff were not sure of exactly what their responsibilities were as to IT security. As noted by the RCMP ‘a strong management culture which proactively supports IT security usually has an organization which is more IT security conscience’.

Benefits associated to an awareness program - Some benefits of a formal IT security awareness session include the transmission of current policies, practices and responsibilities. With HRDC’s ventures into more web based technology and products, such as electronic commerce and Public Key Infrastructure, awareness of IT security becomes even more important. A number of interviewees told the IAB that an HRDC IT security awareness program should be extended to 3rd party deliverers and provincial employees within the LMDA.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

MANAGEMENT OF LOGICAL ACCESS (1)

Many access control processes

- Most national applications have unique access control process

Many people involved

- Access control coordinators are located at NHQ, RHQs, ITCs and HRCCs for different systems (ISP, Labor, CMS, EI, HRIB)

Embedded security

- Security coding has been (ICCM) and continues to be (CMS) embedded in applications
  - minimizes effectiveness of Easylock security software

Logical access control process is diffuse - The logical access control process varies throughout the department as several procedures and software products (Easylock, Top Secret and LAN operating systems) are used by different access control coordinators located in different sites for different systems. This variance leads to excessive administrative overhead and inefficiencies.

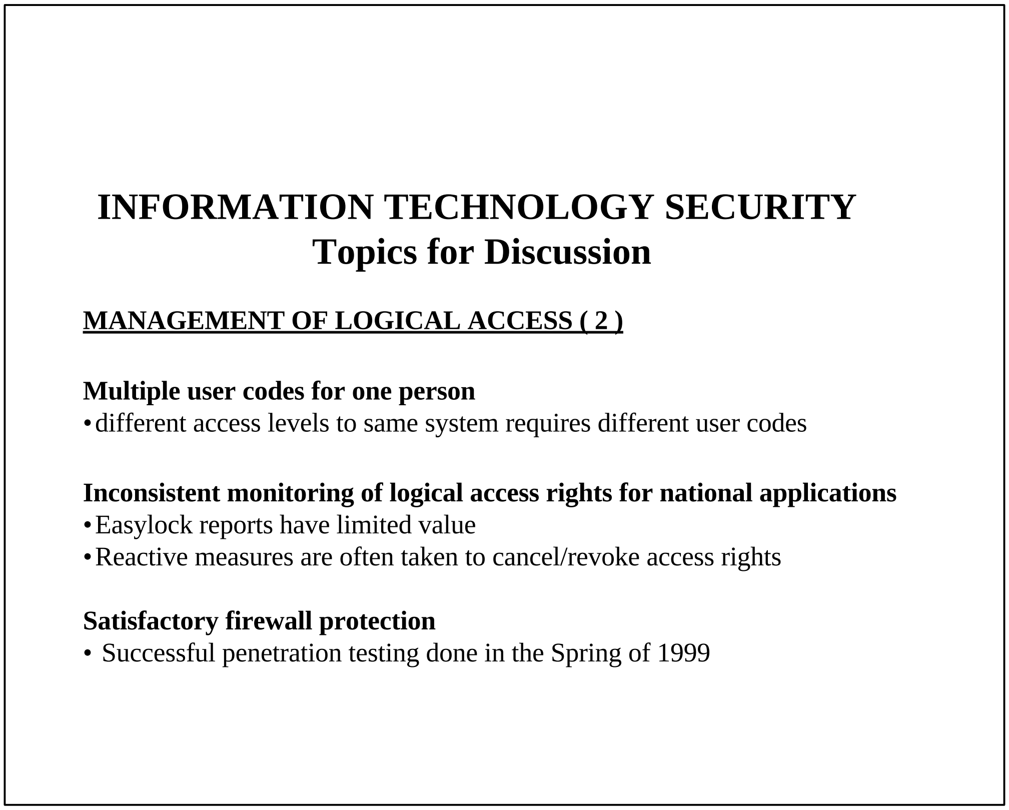
The process to grant the user-ID, passwords and specific access rights to corporate applications varies in each organization - The procedures for processing user codes/passwords to access mainframe (M/F) applications vary depending upon the system/organization. Access control coordinators are assigned to specific national applications. They are located in NHQ, RHQs, ITCs and HRCCs. As indicated in the Structure and Organization chapter, the administration for access codes/passwords for both corporate applications and LANs is fragmented across HRDC. Following are examples of the variations for access requests

- EI and HRIB M/F applications are sent directly to the ITC Security Coordinators from authorized HRCC and RHQ managers while requests for access to CMS are first sent to a regional coordinator for review, then forwarded to the ITC Security Coordinators.

- ISP's Canada Pension Plan (CPP) and Old Age Security (OAS) applications are sent to regional ISP Security Access Control Officers (SACOs), who work independently from the ITCs. These regional SACOs ultimately send these requests to NHQ (Systems/Operations-Security).

- Applications for the Labour Officer Information System (LOIS) and Labour Mobile Adjustment Officer (LMAO) systems, while not M/F applications, are sent to one of five Regional Data Base Administrators (RDBAs), who are also separate and work independently from the ITCs EasyLock's effectiveness.

Access rules and control structure embedded in corporate applications - Prior to Easylock, access rules and control structures were embedded inside national applications such as ICCM. To take advantage of Easylock's single sign on feature, pre-Easylock applications will require embedded security functions to be converted into EasyLock. Currently, applications such as CMS could still be further developed to maximize Easylock's effectiveness. Industry practices indicate that 'security' should be managed by security systems, such as Easylock, not the application.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

MANAGEMENT OF LOGICAL ACCESS (2)

Multiple user codes for one person
- different access levels to same system requires different user codes

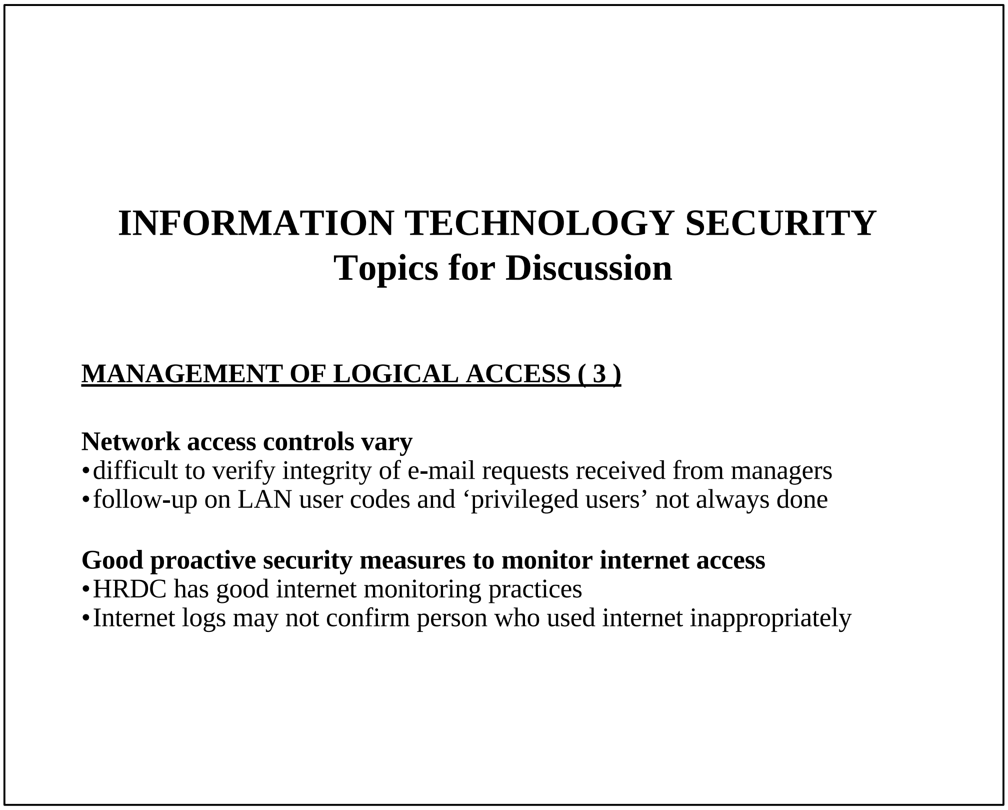
Inconsistent monitoring of logical access rights for national applications
- Easylock reports have limited value
- Reactive measures are often taken to cancel/revoke access rights

Satisfactory firewall protection
- Successful penetration testing done in the Spring of 1999

Multiple User Codes - In addition, each corporate application has its own user-ID, passwords and access restriction. For some staff, they need different access levels to systems (e.g. ICCM) to do their job, resulting in multiple user-IDs/passwords for one person. The absence of single user-ID and password to access corporate application has contributed to the proliferation of user-IDs and passwords across HRDC. Easylock's attributes need to be better utilized when developing applications/systems.

Inconsistent Monitoring - For national applications using the Unisys M/Fs, the ITCs are to produce monthly Easylock reports itemizing users by responsibility center, application used and the last date of password change. However, not all ITCs produce the Easylock report on a monthly basis. Most recipients of the Easylock report claim it has minimal value due to its limited content and wanted the report to also identify the application profiles/roles for each user. For instance, regional CMS coordinators said it would help to know which screens (defined as a "role" in CMS) each user can access. This level of detail would allow an assessment of whether the user had conflicting access levels to the same or different systems, allowing the user to compromise the system(s) and/or engage in fraudulent activities. The IAB was informed that previous reports (e.g. Reporter III) did identify profiles/roles per application and allowed regions to delete old user profiles and add new ones, ensuring capabilities across applications would not be compromised. Due to its usefulness for IT security purposes, one region still requests this report on an annual basis.

Reactive measures are common to rectify logical access rights. The current process is decentralized to the responsibility center manager, who is to inform all responsible parties (such as finance, personnel, IT, etc.) for the movement of personnel. While many LAN Administrators said that they could follow up on inactive user codes/passwords, they indicated that reports, which indicate inactive user codes/passwords, are not readily available. The process needs to be formalized to ensure that HRDC revokes or modifies logical access rights on a timely basis.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

MANAGEMENT OF LOGICAL ACCESS (3)

Network access controls vary
- difficult to verify integrity of e-mail requests received from managers
- follow-up on LAN user codes and ‘privileged users’ not always done

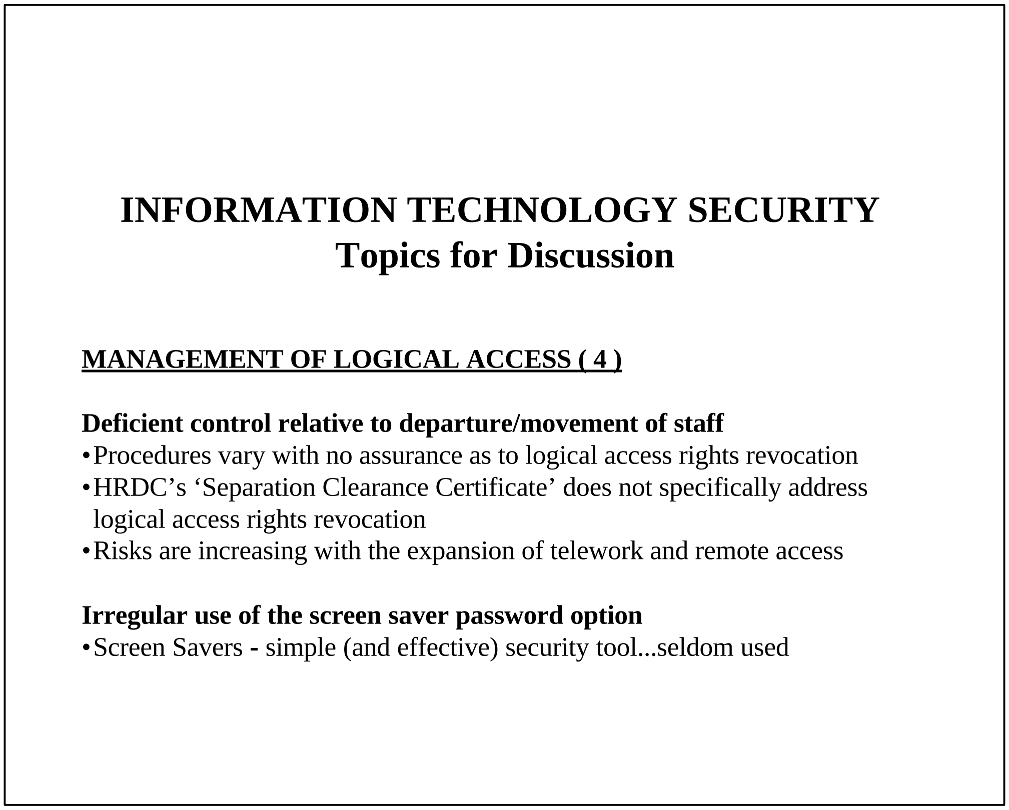
Good proactive security measures to monitor internet access
- HRDC has good internet monitoring practices
- Internet logs may not confirm person who used internet inappropriately

Integrity of e-mail requests - Managers often send e-mails to the appropriate authorities (e.g. Labour RDBA, ISP SACO, ITC Security Coordinators) asking that a particular staff member be given a certain access level to a specific application. The IAB was told that only authorized managers/LAN Administrators (and a few select others) could send these e-mails. Due to their geographical dispersion, the appropriate authorities can not always verify the integrity of these e-mails; most are taken ‘as is’ and processed accordingly. However, the IAB noted that it is common for these authorized managers to give their passwords to a colleague, such as an Administrative Assistant, to monitor incoming e-mails during the manager’s absence. This practice could allow an unauthorized person to send an e-mail to the appropriate authorities requesting access to an HRDC application. HRDC has an e-form, which could help resolve this situation. However, this e-form is not yet capable of supporting ‘digital signatures’ for verifying the originator.

Follow-up on LAN user codes - Some LAN Administrators review the list of users who have access to their LANs, some do not. No LAN Administrator was aware of any functional guidelines on the frequency of reviewing LAN access lists/logs. Managers are supposed to inform their LAN Administrators when a change in an employee’s status necessitates a change in that employee’s LAN access rights/level. However, this does not always happen. One LAN Administrator told the IAB that the main method of finding out about changes to an employee’s status or LAN access rights/level is at the employee's ‘going away’ or ‘promotion’ party. Unfortunately, not all LAN Administrators are invited to these parties, particularly in larger offices.

Follow-up on 'privileged users' - 'Privileged users' are primarily systems staff that require exclusive access rights to HRDC's M/F software, operating systems and corporate applications to undertake technical work (e.g. database management). ITC representatives told the IAB that reports are not presently formatted to indicate which 'privileged' user codes have not been used for extended periods of time. Production of such reports would allow ITC security to follow up with the manager/user to ensure the integrity of dormant 'privileged' user codes. Likewise, there is no assurance that the above situation is any different among Labour (LOIS) and ISP (CPP, OAS) systems. It is the IAB's understanding that Infrastructure could format/produce such reports, if requested to do so.

Monitoring of Internet - be careful with the statistics produced - Most regions have Netscape installed directly on the desktop workstation (hard drive) as opposed to being centrally available from the LAN server. This former practice allows any user to access the internet at any workstation by bypassing ('cancel') the logon procedure. In these circumstances, audit logs can identify which computer (IP address) accessed a web site but not which user, since the 'user ID' process ('log-on') did not occur. One of the region visited installed Netscape on the LAN server. For any user that requires access to the internet, a formal logon process has to take place, thus identifying the user (unless the user has given out his/her user-id and password).



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

MANAGEMENT OF LOGICAL ACCESS (4)

Deficient control relative to departure/movement of staff

- Procedures vary with no assurance as to logical access rights revocation
- HRDC's 'Separation Clearance Certificate' does not specifically address logical access rights revocation
- Risks are increasing with the expansion of telework and remote access

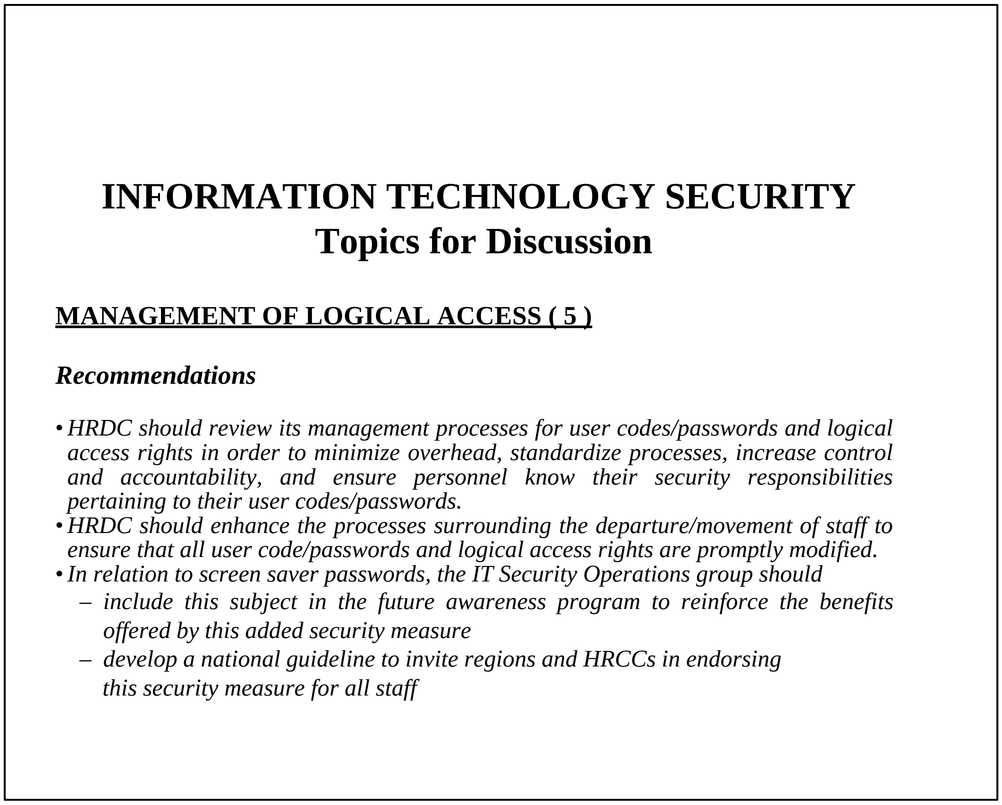
Irregular use of the screen saver password option

- Screen Savers **-** simple (and effective) security tool...seldom used

Departure/Movement of Staff - The procedures associated with the departure/movement of staff does not provide the assurance that, if required, their logical access rights have been revoked or modified. The current separation process is centered around the 'Separation Clearance Certificate - form ADM 5017'. The IAB's review of this process revealed that this form makes no specific reference to IT such as ensuring that departing employees have their logical access rights amended, if required.

All HRDC employees have access to the internet and many have remote access rights allowing them access to e-mail, internet or corporate applications for telework. There is an urgent need to ensure that all these accesses are expeditiously modified as required due to a change in the employee's status.

Screen savers are electronic tools that provide good security measures if they are used conjointly with the 'password' option feature. When screen savers are used, access to unattended desktop or laptops is denied unless a legitimate password is entered to deactivate the screen saver. The IAB noticed that the password feature was frequently left to the users' discretion and often not applied. In one region, users were required to use the 'Microsoft/Window 95/screen saver option' as opposed to using personalized screen saver software. In addition to providing extra security, this HRDC approved screen saver simplified the architecture and standardized the products.

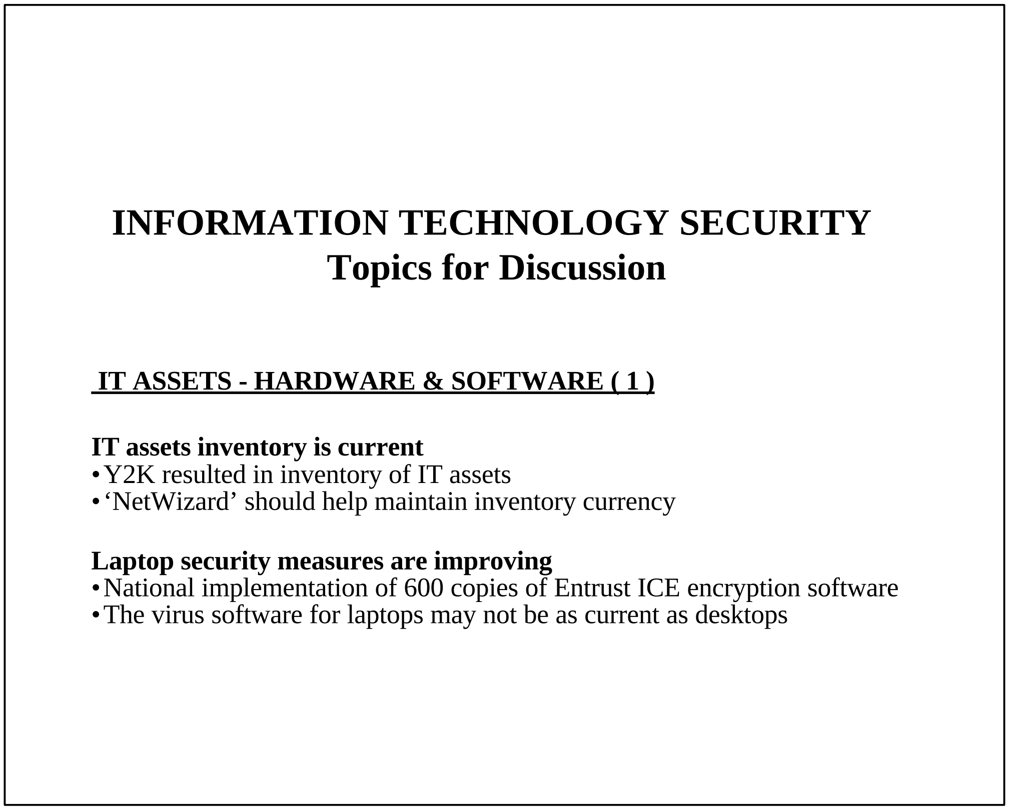


INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

MANAGEMENT OF LOGICAL ACCESS (5)

Recommendations

- *HRDC should review its management processes for user codes/passwords and logical access rights in order to minimize overhead, standardize processes, increase control and accountability, and ensure personnel know their security responsibilities pertaining to their user codes/passwords.*
- *HRDC should enhance the processes surrounding the departure/movement of staff to ensure that all user code/passwords and logical access rights are promptly modified.*
- *In relation to screen saver passwords, the IT Security Operations group should*
  - *include this subject in the future awareness program to reinforce the benefits offered by this added security measure*
  - *develop a national guideline to invite regions and HRCCs in endorsing this security measure for all staff*



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

IT ASSETS - HARDWARE & SOFTWARE (1)

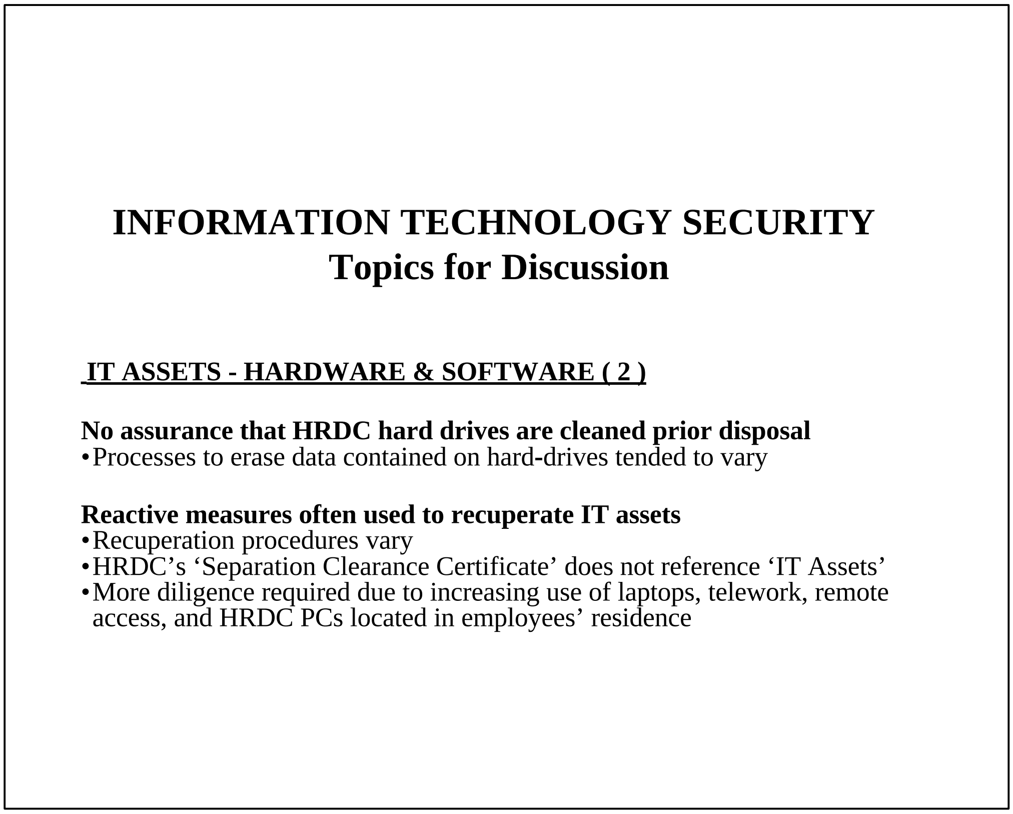
IT assets inventory is current
- Y2K resulted in inventory of IT assets
- 'NetWizard' should help maintain inventory currency

Laptop security measures are improving
- National implementation of 600 copies of Entrust ICE encryption software
- The virus software for laptops may not be as current as desktops

Currency of IT assets inventory - One of the results of HRDC's Year 2000 project was the production of an HRDC inventory for IT assets. The main challenge now is to maintain the inventory's accuracy. To assist in this process, NHQ has selected NetWizard, a software tool that will facilitate inventory maintenance. HRDC is in the process of implementing NetWizard.

Laptop security - The perception of security measures associated to laptops varies among HRDC staff. The IAB noted that HRDC's Security Policy and Procedures Manual devotes a section to Telework in which security measures are discussed pertaining to the use of laptops and the information they contain. However, specifics such as data encryption for hard drives and e-mail attachments are not mentioned. It is the IAB's understanding that HRDC is presently testing Entrust ICE and RSA SecurPC for hard drive encryption.

Concerns were expressed as to the currency of the virus protection software on laptops. Some people reported that laptops were not upgraded with the same diligence as desktop workstations and servers. Many interviewees indicated that they were not aware of any specific departmental policy related to laptops even though HRDC's Security Policy and Procedure Manual contains a specific section on 'laptops'.



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

IT ASSETS - HARDWARE & SOFTWARE (2)

No assurance that HRDC hard drives are cleaned prior disposal
- Processes to erase data contained on hard-drives tended to vary

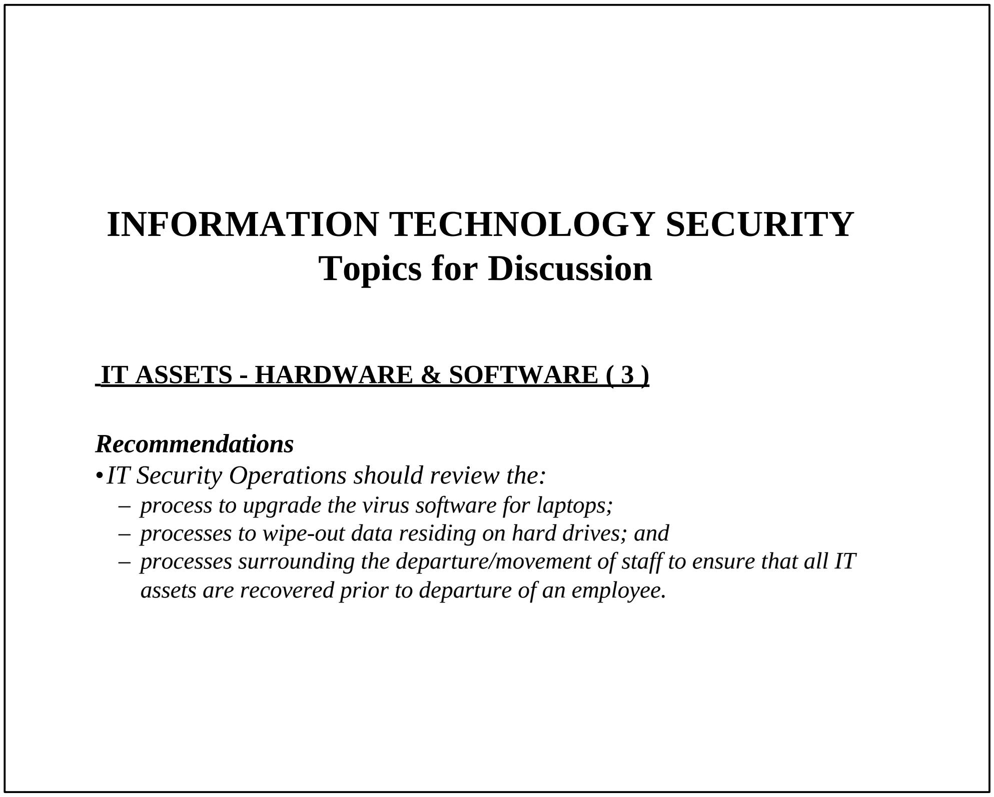
Reactive measures often used to recuperate IT assets
- Recuperation procedures vary
- HRDC's 'Separation Clearance Certificate' does not reference 'IT Assets'
- More diligence required due to increasing use of laptops, telework, remote access, and HRDC PCs located in employees' residence

Cleaning Hard Drives - To keep abreast of recent technology, HRDC regularly replaces desktop workstations, laptops and servers. Prior to disposing of the equipment, it is important to ensure that the information contained on the hard drives be removed. There is no assurance that all hard drives are erased of potentially sensitive HRDC data prior to disposal since the degaussing or 'cleaning" process is inconsistently practiced within HRDC. The assessment revealed that different procedures were used and in some cases, the interviewee was unsure if there was a formal procedure in place.

When the IAB requested HRDC's policy on this issue, NHQ provided us with a copy of the 'Procedure for Wiping Protected Information on Hard Disks, Employment and Immigration Canada, September, 1992'. No one at any of our regional or local site visits was familiar with this document.

Reactive measures often used to recuperate IT assets - Once an employee leaves a responsibility center (RC), it is common for an RC manager to realize 'after the fact' that the employee may be in possession of a laptop computer or other IT asset. Upon leaving an RC, employees are required to ensure that the 'Separation Clearance Certificate - form ADM 5017' is completed. RC managers use this form to acknowledge that the employee has returned calling cards, security passes, locks/keys, etc. However, this form does not make specific reference to IT assets. Therefore, it is not uncommon for someone to terminate their employment with HRDC and still be in possession of a laptop, printer, remote access software, etc. One case where a former HRDC employee was asked to return a laptop, after leaving the employment of HRDC claimed to have already done so; this laptop was never recovered.

Considering today’s operations, it is not unusual for employees to have in their possession an HRDC laptop, desktop or other IT equipment located at the employee’s residence. To ensure that appropriate actions are taken on a timely basis, the process for controlling these IT assets needs to be formalized to ensure that HRDC recuperates IT assets.

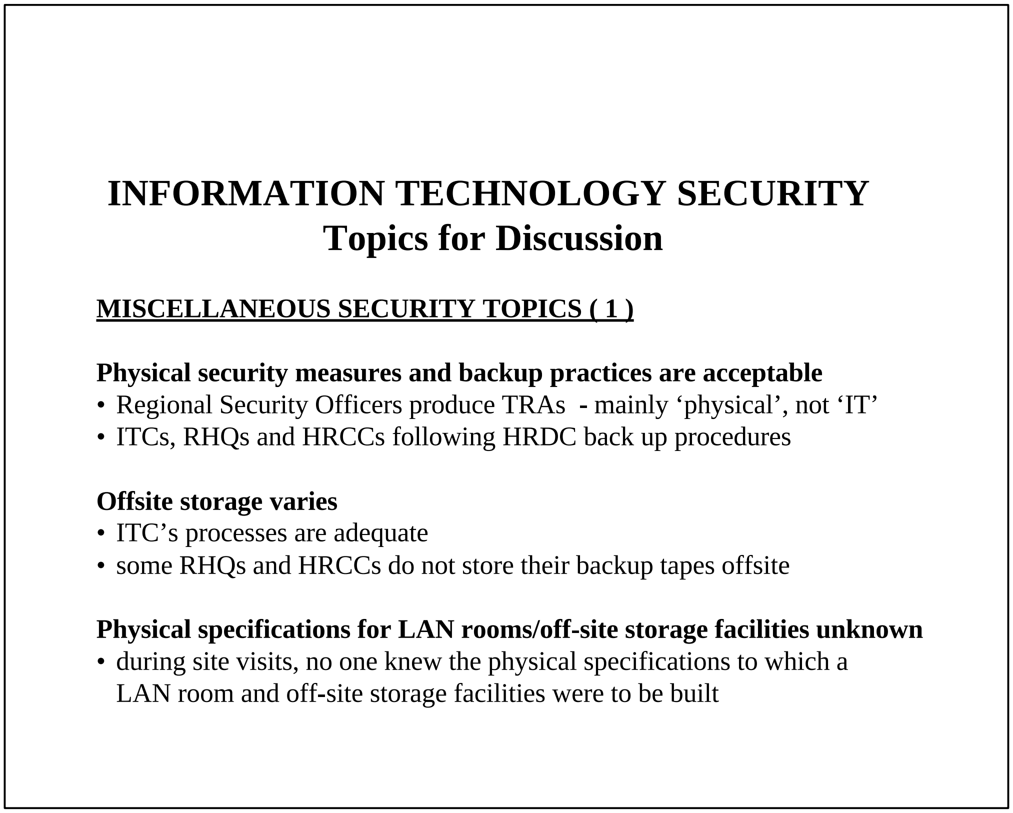


INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

IT ASSETS - HARDWARE & SOFTWARE (3)

Recommendations

- *IT Security Operations should review the:*
  - *process to upgrade the virus software for laptops;*
  - *processes to wipe-out data residing on hard drives; and*
  - *processes surrounding the departure/movement of staff to ensure that all IT assets are recovered prior to departure of an employee.*



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

<u>MISCELLANEOUS SECURITY TOPICS (1)</u>

Physical security measures and backup practices are acceptable
- Regional Security Officers produce TRAs - mainly ‘physical’, not ‘IT’
- ITCs, RHQs and HRCCs following HRDC back up procedures

Offsite storage varies
- ITC’s processes are adequate
- some RHQs and HRCCs do not store their backup tapes offsite

Physical specifications for LAN rooms/off-site storage facilities unknown
- during site visits, no one knew the physical specifications to which a LAN room and off-site storage facilities were to be built

Physical Security - Previously, TRAs were not always completed for HRDC IT projects. Since NHQ’s IT Security Coordinator is part of the Project Review Committee (PRC), all PRC projects will now be reviewed for IT security compliance and concerns. However, there is no assurance that a TRA will be done for other IT projects which are not part of the PRC’s agenda.

At the regional and local level, the RSOs complete the TRAs as requested by their respective RHQ/local offices. They reported that these TRAs are mainly addressing physical security issues and that the IT component is often not addressed. In two regions visited, the TRA template included in the regional Security Policy and Procedures Manual is used as a guide to produce the TRA. One region has planned to conduct TRAs this year in ten different HRCCs.

TRAs that include an IT component are usually more complex to produce since they require a certain technical level of IT expertise which most RSOs do not possess. The regional Security Policy and Procedures Manuals state that “the Regional IT Security Coordinator will complete TRAs”, However, since regions believe they do not have such a person as part of their regional organization, IT risks and vulnerabilities are not identified as well as they could be through the TRA process at the regional and local level.

HRDC recently issued a new LAN operation policy requiring a 20 day back-up cycle and off-site storage. The IAB noted that the regions visited are in various stages of implementing this policy.

While at the RHQs, local offices and ITCs, the IAB visited several LAN rooms and ITC off-site storage facilities. As a result, the IAB witnessed many different physical security measures.

Based on the audit team’s opinions, each location appeared to have satisfactory physical protection mechanisms. However, no one was able to identify or produce national physical security standards and guidelines for constructing LAN rooms and ITC off-site storage facilities. Such standards would be useful to assist in creating LAN rooms, selecting off-site storage facilities, and conducting IT security reviews and TRAs.

INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

MISCELLANEOUS SECURITY TOPICS (2)

IT security breach

- The term ‘IT security breach’ has not been specifically defined
- An ‘IT security breach’ may not always be reported

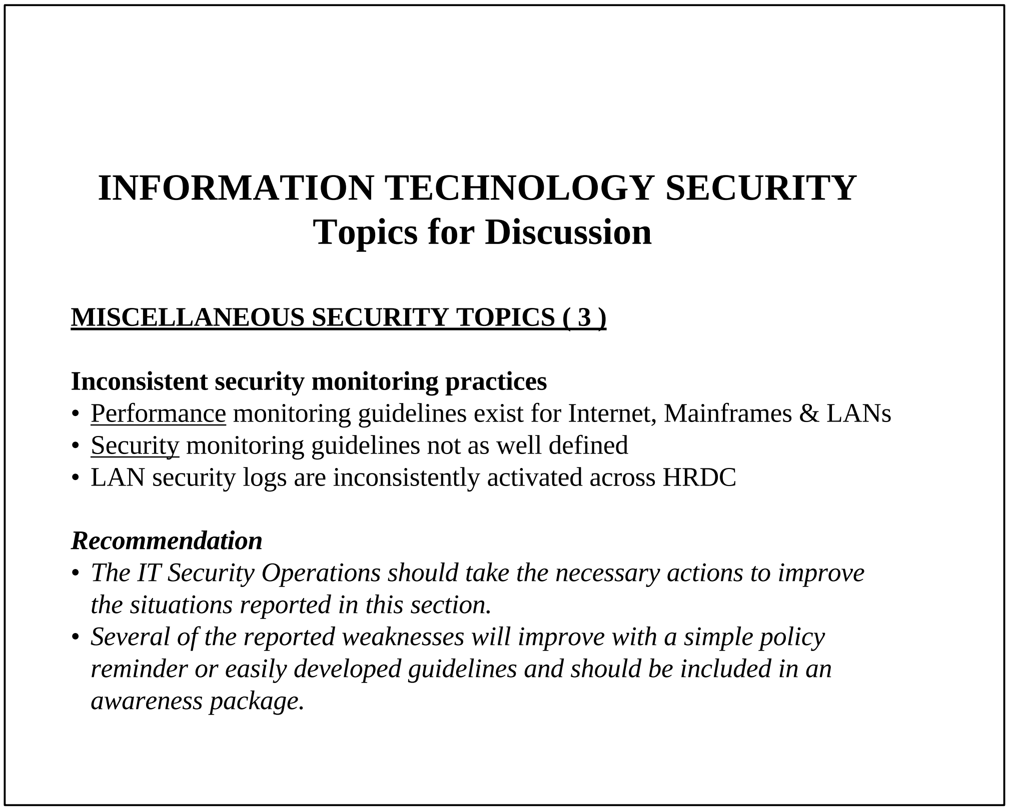
Personnel (hiring)

16(2)(c)

The definition of IT security breaches has not been clearly articulated and a systematic process to report them has not been developed. When asked to define and describe their interpretation of an ‘IT security breach’, people did not know exactly what this term meant or how to report it. The IAB noted that in all of HRDC’s regional Security Policy and Procedures Manual (TRA Checklist, Section G, IT Security, #2. LANs) the question is asked *“Are security concerns and incidents reported to IT security?*” However, since regions believe they do not have a regional IT Security Coordinator, most were unsure how to handle such incidents. Consequently, the IAB concludes that many HRDC IT security breaches may not be documented, reported or accounted for although Treasury Board’s GSP policy states that security breaches (including IT) ‘must be reported to the deputy head of the institution’.

Most HRDC’s personnel are security cleared to the Enhanced Reliability Clearance (ERC) level. This allows access to ‘Protected B’ data on a “need to know” basis. Treasury Board guidelines state that ERCs must be performed for all staff although the ERC process can be bypassed for students and short term employees (less then six months).

16(2)(c)



INFORMATION TECHNOLOGY SECURITY
Topics for Discussion

MISCELLANEOUS SECURITY TOPICS (3)

Inconsistent security monitoring practices

- Performance monitoring guidelines exist for Internet, Mainframes & LANs
- Security monitoring guidelines not as well defined
- LAN security logs are inconsistently activated across HRDC

Recommendation

- *The IT Security Operations should take the necessary actions to improve the situations reported in this section.*
- *Several of the reported weaknesses will improve with a simple policy reminder or easily developed guidelines and should be included in an awareness package.*

There is a lack of consistency related to IT security monitoring and review as there is no national and/or regional guidelines on this matter.

Network operational logs are electronically produced, such as sites accessed through the Internet, data files accessed by workstations, users logon results and response time statistics. Aside from the LAN performance logs being closely monitored, IT security logs are not monitored on a regular basis. Some LAN Administrators said they did not activate security logs at the server level since they ‘had no IT security problems’. However, these same LAN Administrators conceded that they could not substantiate that they ‘had no IT security problems’ since they did not produce and monitor LAN audit/security logs. Likewise, no LAN Administrators knew of any functional guidelines or policies indicating which specific LAN audit/security logs should be maintained and how long these LAN logs should be retained.

IT security logs are useful to produce statistics which can be analyzed to detect trends, and assist in the investigation of IT security breaches. The Québec region’s RSO works closely with the Montréal ITC Security Coordinator and frequently uses current and special request IT logs to investigate frauds. Last year, the RSO uncovered 75 fraud cases which were perpetrated through the misuse of IT. It is the IAB’s belief that if other regions also used IT audit/security logs more diligently to identify frauds, similar results would be achieved.

APPENDIX A

FEDERAL GOVERNMENT'S IT GOVERNANCE FRAMEWORK

BACKGROUND

The Need To Implement the Security for IT

During the past decade, the federal government has greatly accelerated its investment in information technology (IT). This has led to significant pay back in terms of greater public service productivity, increased international competitiveness in the new global economy, and most importantly, improved service to Canadians.

It is important to note, however, that this investment has not come without new risks. Just one example, is the trend of continuing migration of computing power from centralized systems to the desktop and beyond, to the point of service. Many safeguards, which had matured in the closed system, mainframe computing environment, still do not have equivalents in the new open architecture, client/server environment. Thus, valuable information and services reliant on IT, once reasonably protected from losses of confidentiality, integrity and availability, are now at more risk.

It is therefore, critically important that departments fully implement the Government Security Policy and IT Security operational standard.

GSP Monitoring Requirements

The Government Security Policy (GSP) was first issued in June 1986. It was revised in 1987, and again in January 1990. The policy will be revised and extended in early 1994. Some of the new Information Technology Security (ITS) requirements, such as those related to Network Security, reflect the risks being introduced by these new technologies.

One of the primary requirements of the GSP is that of monitoring. This is usually accomplished through the performance of periodic audits.

Departments are required to conduct an internal audit of:

- their compliance with the policy; and
- the effectiveness and efficiency with which they are implementing it, at least once every five years, the first to have been completed by the end of 1993.

Although the requirement for auditing of the whole of the GSP is minimally once every five years, rapidly changing areas such as ITS should be audited more often, where practicable.

Treasury Board Secretariat (TBS) is reliant upon these audits, as well as upon reports issued by the RCMP, the Communications Security Establishment, the Public Service Commission and the National Archives, in order to monitor departmental compliance with the GSP.

HRDC Internal Audit Branch in conducting audits of the implementation of the GSP and the ITS operational standard.

HRDC - IAB auditors propose to assess, in a broad sense the:

– departmental compliance with the Security Policy and ITS operational standard;
– effectiveness of implementation of the Security Policy and ITS operational standard; and
– efficiency of implementation of the Security Policy and ITS operational standard.

For the purposes of this document, the following definitions are utilized:

– effectiveness is achieving stated objectives or planned service levels with a minimum of negative outcomes. To be effective, an ITS program or activity must also remain relevant; and
– efficiency is achieving desired results with the least resource cost. Efficiency reflects the relationship between the resources used (dollars, person-years, information and other assets) and the results achieved.

More specifically, the audit objectives, criteria, and procedures will help auditors assess:

– whether an adequate organization and administration structure exists to support the ITS environment;
– whether formal and appropriate policies, practices and procedures exist for the ITS environment;
– whether an adequate security risk management framework exists for the IT environment; and
– whether management is achieving an appropriate economy in the ITS environment.

SECURITY ENVIRONMENT

Accountability Framework - A fundamental principle of the GSP is the accountability of deputy heads for security within their departments. Both the policy and the operational standards outline requirements with which departments must comply. The operational standards also include recommended safeguards to apply unless a threat and risk assessment (TRA) indicates otherwise.

Departments may exceed standards by adding safeguards that the deputy head considers necessary to protect sensitive information and assets.

If departments are to implement programs that are efficient and effective, they must be able to administer them within their particular mandates and according to their priorities, budgets, and organizational cultures and environments. The policy recognizes this by defining broad requirements to ensure a certain level of security throughout government or a department, while allowing the discretion needed to respond to financial and other conditions.

The Government Security Model - The government security standards describe a departmental security program model having the following components:

– Organizational Structure;
– Administrative Procedures; and
– Three (3) sub-systems:
    1. Physical Security,
    2. Information Technology Security, and
    3. Personnel Security.

The effectiveness and efficiency of the overall security program depends upon the performance in each of these sub-systems. Therefore, where responsibility for the various sub-systems is assigned to different organizational units, or where it is decentralized, the sub-systems should be structured to support cooperative planning, management and administration.

The ITS Model - ITS is often described as the protection resulting from an integrated set of safeguards designed to ensure the confidentiality of the information electronically stored, processed or transmitted; the integrity of the information and related electronic processes; and the availability of systems, networks and services.

The ITS operational standard describes a model with the following components:

– Organization and Administration;
– Operations; and
– Seven (7) other sub-elements:
    1. Personnel Security;
    2. Physical Security,
    3. Hardware Security,
    4. Software Security;
    5. Communications Security;
    6. Emanations Security; and
    7. Network Security.

The effectiveness and efficiency of the ITS security program depends upon the performance of each of these sub-elements. Therefore, where responsibility for the various security sub-elements is assigned to different organizational units, such as to an EDP Security unit and a COMSEC unit, or where it is decentralized, the sub-elements should be structured to support cooperative planning, management and administration.

ITS is most effective when it is accepted as just one of the many important requirements that system developers and maintainers need to consider. ITS is not an "add-on". It should be viewed as an integral component of any given IT infrastructure. When properly managed, it provides system and data owners with a return on investment.

ROLES AND RESPONSIBILITIES

1. **Senior Security Representative** - Departments are required to appoint a senior official to represent the deputy head in dealings with TBS about the Security policy and standards. The appointed official does not necessarily need to be the Departmental Security Officer (see below).

2. **DSO** - Departments must also appoint a Departmental Security Officer (DSO). The DSO is responsible for developing, implementing, maintaining, coordinating and monitoring a departmental security program consistent with the Security policy and standards.

3. **ITS Coordinator** - Departments must appoint an IT Security Coordinator. This position should have at least a functional relationship with the Departmental Security Officer (DSO). Previously, the ITS Coordinator was referred to as the EDP Security Coordinator; this title may still be used, if the department wishes.

4. **COMSEC Authority** - Coordination of emanations and cryptographic security should be embodied in the role of a (Communication Security Officer) COMSEC authority. The role may be filled by the ITS Coordinator, a person in a separate position, or by CSE acting on behalf of the department.

5. **ITS Lead Agencies** - There are two lead agencies for ITS: the RCMP and CSE. The RCMP Security Evaluation and Inspection Team (SEIT) carries out inspections of IT security, as per the schedule in the ITS operational standard. CSE inspects, tests and evaluates COMSEC systems and procedures. Also, CSE's National Central Office of Records (NCOR) audits departmental COMSEC accounts; after which, it issues a report with recommendations to the deputy head or chief executive officer.

Inter-Departmental ITS Committees - There are two inter-departmental ITS committees that deal specifically with ITS issues. The Communications Security Committee provides strategic direction to participating departments on the management of COMSEC material and systems. The ITS Committee advises the RCMP, CSE, and TB on ITS.

Risk Management Framework - The Security policy requires departments to assess threats and risks to which sensitive information and assets are exposed, select risk-avoidance options, implement cost-effective safeguards, and develop contingency and business resumption plans, as required. A department's IT system development life cycle methodology should include the appropriate steps for:

- assessing threats and risks to IT assets; and
- choosing, certifying, accrediting, maintaining, monitoring and adjusting safeguards.

When properly implemented, the security risk management process will confirm the need for minimum safeguards and show the need for additional types or levels of safeguards. It also provides value-added in that it increases awareness and support for the ITS program.

INFORMATION TECHNOLOGY ISSUES - TRENDS

As public and private sector IT systems and networks become more prevalent, decentralized, and interconnected while their use becomes more unconstrained, society becomes more vulnerable to increased threats that can cause losses in data confidentiality, integrity and availability. Many trends underlie this audit; ten (10) of which are detailed below.

Although these trends apply to both the public and private sectors, some have been described more from the public sector point of view. IT has been spreading outward, to change all aspects of government services - from inspections at client sites to automated self-service centers. From an ITS point of view, it is important to understand these changes; identify any new vulnerabilities and threats which may have been brought with them; and then offset any unacceptable risk through safeguard definition, selection, application and monitoring.

1. **Increasing end-user expertise** - Users are becoming increasingly knowledgeable about computers and telecommunications. Although in one sense, this is very positive, in that it fosters a highly productive IT environment, it also comes with a down-side. It has been long said that "a little knowledge can be a dangerous thing". This is no less true in the computing and telecommunications environment. Technology-literate individuals, bent on subverting and disrupting IT systems and their data, are able to do so with sometimes relative ease. Yet, it is also important to note, that at the same time, we are also witnessing an increase in more sophisticated system and network attacks.

2. **Rapidly changing and increasing complexities of the IT environment** - Experts have stated that world information is now doubling approximately every four years. This is expected to decrease to every 18 months, by the year 2000. With this acceleration, comes the need for IT to do more, do it faster, and do it better. New product and service offerings are being released by high technology companies at a rapid pace.

   IT is frequently updated or replaced. A security audit should ensure that threat and risk assessments (TRAs) are updated upon major changes in the IT arena.

   Also, it is becoming increasingly difficult for IT personnel, and especially ITS personnel, to remain current of all this change and complexity. Most ITS personnel are IT specialists first, and security specialists, second. Suitable and continuous training in both fields must be in place.

3. **Computing power migration** - One of the most significant trends is the migration of computing power from centralized government systems to the desktop and beyond, to the point of service. Control over technology has moved from the central Informatics group outward, throughout the organization. HRDC is no any different. Several players have become involved in IT plans, strategies, and acquisition and implementation decisions. Individuals no longer work in isolation: through networking, the group has become the mainstay work unit.

But all of this empowerment, and resulting higher productivity and quality levels has not come without new challenges. Problems still include incompatibility, inability to interconnect, weakened support infrastructures and new and increased security threats and vulnerabilities. Security safeguards, which had matured in the closed system, mainframe computing environment, still do not have equivalents in the new open architecture, client/server environment. This means that valuable information and services heavily dependent on AIT@, once reasonably protected from losses of confidentiality, integrity and availability, are now generally more at risk.

4. **Convergence of networks and computers** - Computers are no longer "islands of processing power" as they once were. Similarly, telecommunication systems are no longer "pieces of wire". Gradually, the two are converging. Now that telecommunications services are digital, they are in effect computers themselves. And the computers controlling these networks are being programmed to provide a wide variety of services. The two elements are fostering a whole new generation of value-added services, such as electronic commerce, video-conferencing; electronic mail and voice mail. This range of services is unlimited, as telecommunications evolves from basic communications to an information utility.

   This change is making it increasingly difficult to determine which organizational unit is responsible for specific ITS areas. It is possible that three or more organizations may be sharing the same responsibilities: the central Informatics organization, the traditional COMSEC organization, and the traditional EDP security organization. As a result, there may be overlap and duplication in the application of ITS; or worse, new ITS threats may carry on unnoticed. This change has resulted in some departments folding the traditional EDP Security and COMSEC organizational units into one ITS unit, to help ensure consistent application and no duplication of services.

5. **Outsourcing** - Outsourcing is the transfer of part or all of the Informatics and telecommunications functions to an outside contractor. It has become increasingly popular, as organizations seek new ways to economize and focus on core business functions. Many large private sector organizations and government departments have already outsourced large components of their IT environment: from operations, to application development to software maintenance. Although outsourcing has many benefits, it also has its drawbacks. These include high costs of exiting and increased executive management involvement. Most importantly, from an ITS perspective, outsourcing means a loss of control. And with this loss of control stems new vulnerabilities and potential threats.

   It is critically important, that before any outsourcing occurs, the security threats and risks are assessed, security requirements are defined, put into the outsourcing contract, implemented and finally certified. Well-tested contingency plans should be in place in case the vendor should not be able to continue to operate. Lastly, the outsourcing contract should allow for regular and surprise inspections, to help confirm that requisite ITS safeguards are in place.

6. **Rightsizing** - Rightsizing is a relatively new trend of reducing an organization's personnel, data centers and facilities in order to achieve optimal productivity. It replaces downsizing, which simply focused on migrating applications from mainframe computers to minicomputers or local area networks (LANs). Rightsizing focuses on the goals of expense reduction and improved client service.

   HRDC must be careful to retain sufficient personnel so that certain duties may be kept separate. In some rightsizing instances, it may be impossible to maintain adequate division of duties in all cases. When this occurs, alternate safeguards should be substituted.

7. **ITS - A selling feature** - Increasingly, ITS in itself, is becoming a selling feature. This is a direct result of several recent trends.

   As part of government restructuring and re-focusing, Organizations, including HRDC, are becoming more client-oriented. They are actively soliciting client needs, in light of particular service offerings. External clients include Canadians and other departments.

   Due to increased media attention, individuals and organizations are becoming much more attune to the threats and risks being encountered in the new electronic global village. The media frequently focuses on computer related problems; such as a computer virus, a computer hacking event, a personal or corporate tragedy caused by computer loss of integrity, or even a loss of a critical service caused by computer outages.

   Canadians and internal government clients have come to expect forever increasing quality of service.

   The combination of these trends creates an environment of clients, insisting on adequate protection for their entrusted information, and expecting full integrity and availability of service offerings heavily dependent upon IT.

   The trend of ITS being a marketable benefit, will likely continue as long as there is substantial outstanding and unacceptable threats and risks in the IT environment.

   Auditors should ensure that IT developers are asking their clients whether security (sometimes expressed by clients as peace of mind or confidence) is a feature that they wish built in.

8. **Increased investment in IT** - The broad government agenda has created the need to constantly improve high quality services to Canadians, yet within an era of restraint. As a result, departments, in looking for innovative ways to meet these challenges, are discovering that substantial gains in productivity, service quality and cost of operations can be found through investment in IT. To this end, the Canadian government spent $11 billion to acquire IT goods and services, between 1986 and 1992. The investment continues to grow, averaging over 8% annually. In 1993 this represented an expenditure of over $2 billion; being equally divided between Informatics and telecommunications.

Without qualified and available support to maintain this IT investment, systems and networks will fail to live up to promises and expectations. Unacceptable losses can quickly transpire. Departments should develop formulas, which help calculate the necessary expenditure of IT support services, including those of ITS. Clearly, the investment in ITS cannot remain static, while overall IT investment accelerates each year, without it causing significant impact.

9. **Shared government systems** - Government policy promotes the move towards common, integrated administrative systems in finance, human resources, assets and materiel. Implementing these systems will take maximum advantage of limited resources, support managers, and will enhance the electronic transfer of information. Shared IT will be used to support infrastructure of the government through such tools as electronic mail, the aforementioned administrative systems, electronic bulletin boards and electronic commerce.

   One effect of this is that the shared system will become extremely distributed. It is estimated that the Public Service Compensation System (PSCS), alone, has the potential to be accessible from over 140 departments, in over 500 physical locations, by over 25,000 public service employees. This has profound implications for ITS. The design, implementation, and maintenance of ITS becomes much more complex. It requires greatly enhanced inter-departmental cooperation to ensure consistent safeguard application, so that very few weak links in the chain exist. One department's insecurity can quickly become the catalyst for loss of another department's critical data, on the shared system.

   Shared-system managers need to clearly analyze and define the ITS safeguards in the shared responsibility domain. User departments should then faithfully implement and monitor those safeguards.

10. **Interconnected systems** - Alliances with other levels of government, business and labour are becoming more of an accepted and widely used model of cooperation. Electronic data interchange (EDI), electronic funds transfer (EFT) and electronic commerce (EC) (in general) are becoming commonplace business strategies. A sub-set of this trend, is the growing need to interconnect government systems and networks with other government and private sector systems to allow transfers of data.

    Departments need to ensure that their system interconnections do not compromise the security profile of their own systems. For example, prior careful analysis, and possibly additional safeguards should be implemented, before a System-High computer processing designated data, can be linked to a Multi-Level computer processing unclassified data.

APPENDIX B

VARIATIONS IN HRDC DELIVERY OF IT SECURITY

Organizational Structure

- Two of the four regions visited have taken the initiative to partner with the ITC Security Officer to deliver a combined Physical and IT Security awareness program whereby the RSOs are actively working with ITC Security to promote IT security during planned site visits.

Planning

- Consequential to most regional and local office people feeling that there is no national vision and strong functional direction for IT security, the IAB noted some movement by some select people to create IT security plans with whatever means were available to them. One example was of a RSO who successfully rationalized an increase in the regional security budget. A portion of the increase is for more site visits at which time IT security will be a prominent part of the visit. Since the RSO does not have a strong IT background, he has been continuously liaising with the Operations IT Security group at the ITC. An informal arrangement now exists whereby the RSO will coordinate his site visits with an IT Security colleague from the ITC at which time, IT security will be comprehensively explained to staff.

Logical Access

- Aware of user code/password variation, different groups throughout HRDC have various initiatives underway to standardize the management of user codes/passwords. One ITC has circulated a draft version of ‘Administrator’s Guide For Managing Mainframe Access At HRDC’ to their region’s LAN Administrators.

- Nationally, an electronic form is planned to ultimately become the common, national process to request user codes/passwords.

- The Montreal ITC and Quebec region, uses a regionally developed process (mainframe) that is similar to the proposed e-form application. However, this process is to be retired due to Y2K. If the e-form for user code/password is not complete prior to this retirement, then the Montreal ITC / Quebec region will need to either Y2K upgrade their automated process, or revert to e-mails or a manual process.

Departure and Movement of Staff

- One HRCC LAN Administrator said the most common way to know of departing employees is at their “going away party”, after which the LAN Administrator would revoke the departing employee’s user code/password. Unfortunately, in bigger offices, such as RHQs, some LAN Administrators are not always invited to a departing employee’s “going away party”.

Monitoring and Review

- One LAN Administrator reported that upon starting his duties, he reviewed the existing HRCC’s IT environment. This review indicated that the previous LAN Administrator gave all HRCC staff access to the System Support for Agents (SSA) Utility. Consequently, all staff had the capability to undertake data base administration functions that should have been restricted to privileged users only. Additionally, this same LAN Administrator reviewed the users of the LAN and found one person who was not an HRDC employee. Apparently, this non-HRDC person was a representative of a third party deliverer who was given access to the LAN and had never been removed. Ironically, this same LAN Administrator no longer reviews LAN usage log for user verification.

- Another LAN Administrator in a different HRCC claimed to do monthly visual inspections of LAN logs and, a result, no documented logs were available for analysis by the IAB. However, another LAN Administrator in a different HRCC documented his monthly inspections.

EasyLock Reports

- One ITC claimed to issue the report bi-monthly but an HRCC LAN Administrator claims to have contacted this same ITC as reports have not been received for a period of four months. Upon review of the report, the LAN Administrator requested the ITC to delete 15 user codes/passwords.

- In a different region, a LAN Administrator claims to not have received these reports for six years and that recently a copy was provided. Upon reviewing the report, more than fifty “requests to delete access rights for former employees” were sent to the ITC.

- One person informed the IAB of being given ‘temporary’ access to Labour’s LOIS database approximately two years ago. Upon completion of the assignment, this person no longer needed access to LOIS and assumed that the ‘temporary’ user code/password had been deleted. However, upon needing access to LOIS two years later, this person learned that the previous ‘temporary’ user code/password was still active.

- The IAB talked with one manager who receives the Easylock report but does not use it since this manager 'doesn't understand it'. This manager has neither taken the time to 'understand' the report nor has anyone followed up to ensure that the report was being properly reviewed and monitored.

- The Easylock Administrator can view ICCM passwords in clear text.

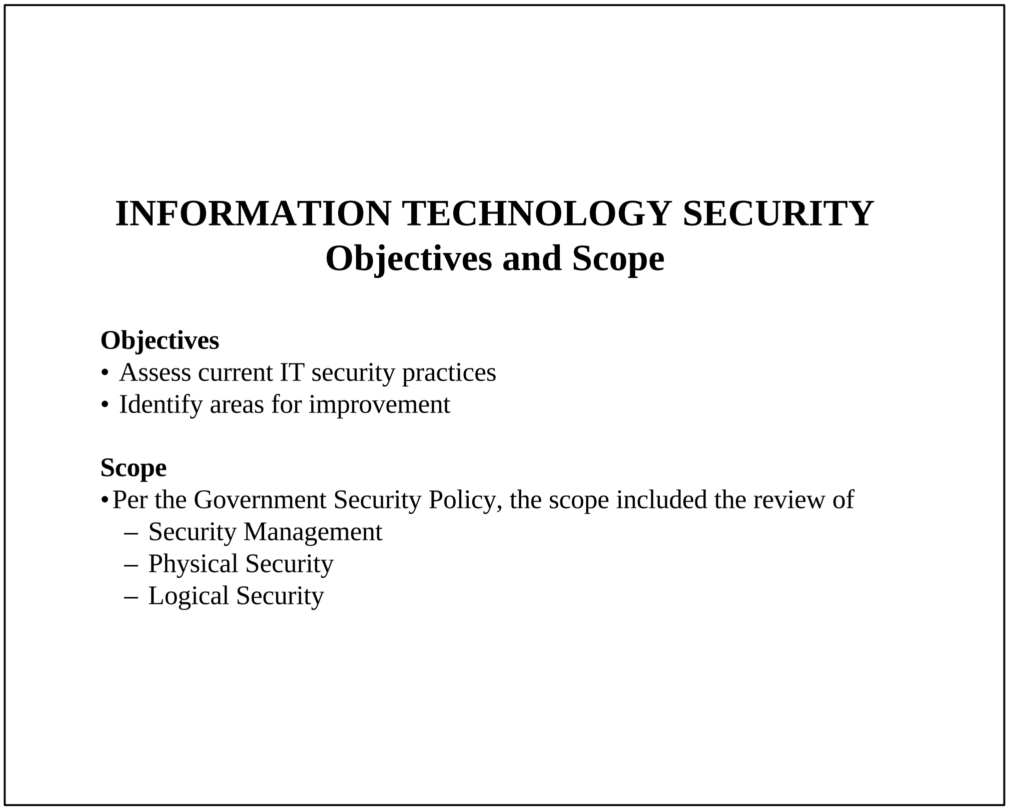
Physical

- The IAB visited one HRCC in which back up tapes were being stored in a fireproof safe. While a fireproof safe would hopefully ensure that paper might not burn, there was no assurance that the heat from a fire would not melt plastic tapes.

- Upon visiting another HRCC, the IAB noted two different brands of tapes being used to perform back ups. The LAN Administrator advised the IAB that he was switching brands to the one he personally used at home since he liked them better. The LAN Administrator said that he was not aware of any HRDC or government standards (e.g. quality/technical specifications) pertaining to the type of tapes to be used for back up.

- One RHQ took LAN backup daily and had sufficient backup cycles. However, the backup tapes were not stored off-site and were not even well secured within the RHQ.

APPENDIX C



INFORMATION TECHNOLOGY SECURITY
Objectives and Scope

Objectives
- Assess current IT security practices
- Identify areas for improvement

Scope
- Per the Government Security Policy, the scope included the review of
  - Security Management
  - Physical Security
  - Logical Security

The objectives of this assessment were:

- Providing management with an opinion on:

  - HRDC's current position against generally accepted IT security practices, the accountability and control frameworks, and
  - how IT security interfaces with HRDC's security governance structure;

- Determining the adequacy of managerial policies, practices and standards and compliance;

- Identifying inconsistencies and risks of major components/processes within all IT security processes and making practical recommendations for improvement.

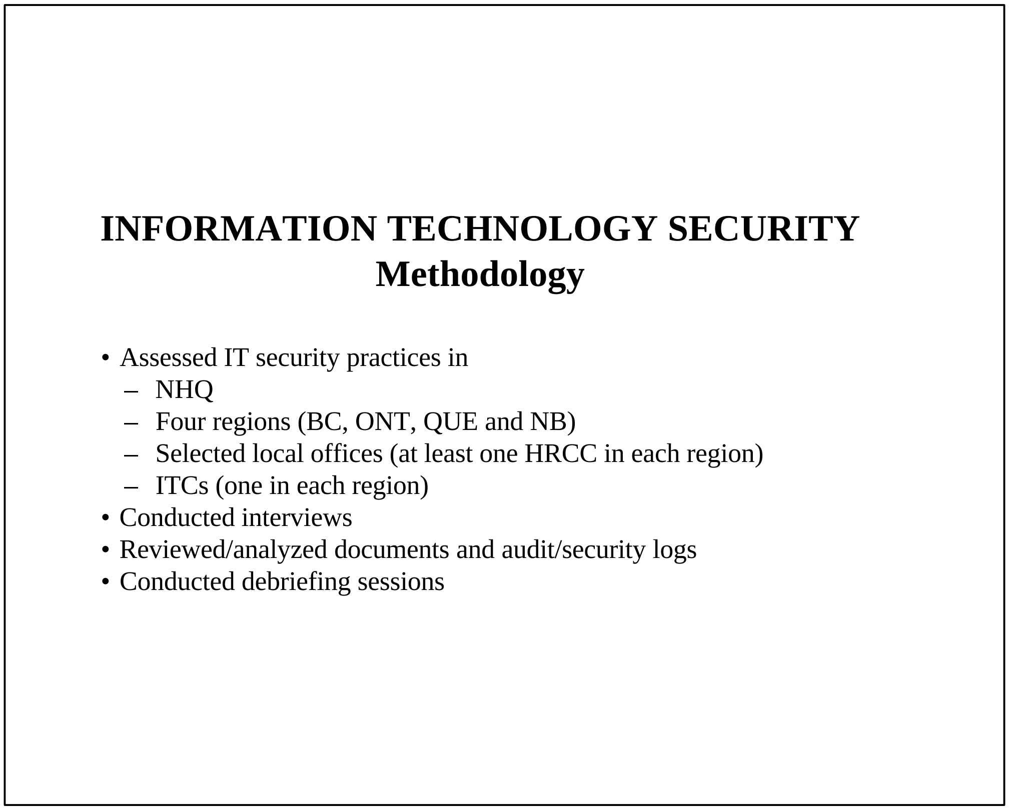
The audit scope was:

- ***Security Management*** - Management Framework - Organization & Structure, Resources, Accountability, Leadership, Planning, Control, Communication, Comptrollership, Performance Indicators, Senior Management Acceptance/Priority/Culture, User Awareness/Culture, Policies and Operational Procedures/Documentation

- ***Physical Security*** **-** Physical security of IT assets/resources - laptops, LAN rooms, off-site storage facilities, restricted access, environmental - temperature control, air purification, Halon gas, etc., Business Resumption Plan (BRP)/Disaster Recovery Plan (DRP) and Contingency Planning (CP).

- ***Logical Security*** **-** Access Paths (e.g. *.*), User ID and Authentication, User codes/ passwords, Access Control Software (e.g. Easylock), File Libraries/Back-ups, File Integrity, PC/Server Security, Main Frame Security, and Firewalls.

APPENDIX D



INFORMATION TECHNOLOGY SECURITY
Methodology

- Assessed IT security practices in
  - NHQ
  - Four regions (BC, ONT, QUE and NB)
  - Selected local offices (at least one HRCC in each region)
  - ITCs (one in each region)
- Conducted interviews
- Reviewed/analyzed documents and audit/security logs
- Conducted debriefing sessions

METHODOLOGY

Research and interviews were conducted with personnel at national headquarters (NHQ) including four (Vancouver, Belleville, Montreal, and Moncton) Information Technology Centers (ITCs), four (British Columbia/Yukon, Ontario, Quebec, and New Brunswick) regional headquarters (RHQ), and one local office within each region. Interviewees included:

- national, regional and local security officers (e.g. Departmental, Regional, and ITC Security Coordinators and Representatives);

- IT management and staff (e.g. NHQ Systems, RSMs, ISP's Security Access Control Officers, Labour's Regional Data Base Administrators, LAN Administrators); and

- Non-IT (ISP, Labour, EI, HRIB, HR, FAS, SPP) management and staff who use IT (hardware, software, telecommunications, national applications/local systems, etc.) on a daily basis to perform their jobs.

- While on site, IAB requested relevant IT security reports/logs such as mainframe access including privileged users, Mainframe security violations, LAN/WAN security violations, and LAN access.

- When these reports where available, IAB, with the assistance of the recipient/generator of these reports, documented the reports' process (e.g. reason/purpose, integrity of information, frequency of production, users, etc.).

IAB also did cursory visual inspections of the physical premises used to secure LAN back-up tapes/files and server rooms. Finally, IAB inspected the facilities used by the ITCs for off-site storage locations.