Comprehensive Audit of HRDC's (SDC & HRSDC) Information Technology Security

Final Report
Project No. 6577/04

Audit and Evaluation Directorate
Policy and Strategic Direction
Social Development Canada

Project Team:

Director General: *J. Blain*
IT Audit Director: *P. LePage*
IT Audit Manager: *M. Winterburn*
IT Team Members: *K. Allen*
F-M. Brière
IT Consultants: *Communications Security Establishment (CSE)*
Electronic Warfare Associates (EWA)

October 2004

SDC-A-003-10-04E
(également disponible en français)

General Disclaimer
Please note that information that would normally be withheld under the *Access to Information Act* or the *Privacy Act* does not appear in the following report.

Paper
ISBN: 0-662-40704-0
Cat. No.: SD34-7/2005E

PDF
ISBN: 0-662-40705-9
Cat. No.: SD34-7/2005E-PDF

HTML
ISBN: 0-662-40706-7
Cat. No.: SD34-7/2005E-HTML

Table of Contents

Executive Summary

As approved by HRDC's Audit and Evaluation Committee (AEC), the objectives of this three-phased Comprehensive Audit of HRDC's (SDC & HRSDC) Information Technology Security (ITS) were to provide departmental senior management with an assessment regarding HRDC's:

1. ITS Governance Framework;
2. Internal ITS Vulnerabilities: On-Site Technical Vulnerability Assessment (OTVA); and
3. External ITS Vulnerabilities: Active Network Security Testing (ANST).

ITS can be briefly defined as the control structure established to manage the integrity, confidentiality, and availability of IT data and resources. This control structure requires an appropriate management framework and governance structure complimented by adequate technological protection. Since the sophistication of attacks on computer systems increases daily, it is virtually impossible for any large IT organization to be completely immune from attacks and its possible consequences all the time; HRDC is no different. Notwithstanding, cognizant of their responsibility to protect HRDC's clients' confidential and personal information, HRDC's senior management authorized this audit to assist them in identifying areas where improvements could be made to HRDC's ITS.

While the audit noted a number of positive attributes within HRDC's ITS environment it also noted a number of areas for improvement. Fortunately, most of the solutions to improve HRDC's ITS are within HRDC's control and simply requires some 'fine tuning' of what already exists.

For Phase I (ITS Governance Framework), conducted primarily from October 2003 to March 2004, the Audit and Evaluation Directorate (AED) assessed HRDC's ITS management, operational, personnel and technical controls in relation to its ITS Governance Framework. As well, HRDC's progress in addressing the issues brought forward in two previous audits (Office of the Auditor General - OAG, April 2002, and HRDC Internal Audit, September 1999) was also assessed.

Phase I concluded that most elements of HRDC's ITS Governance Framework exist such as:

- a Memorandum of Understanding between HRDC's Departmental Security Officer (DSO) and Systems Branch that articulates ITS responsibilities between the DSO and Systems;
- the existence of an ITS Governance Committee;
- a departmental ITS Model requiring ITS issues be addressed throughout the initial and subsequent phases of the Project Life Cycle process;
- proper security clearances for Local Area Network (LAN) Administrators;
- back ups of data regularly occurring; and
- independent confirmation that HRDC responded appropriately to the issues noted in the OAG's 2002 ITS audit.

Some of the areas for improvement include the need to finalize, implement and maintain an ITS awareness program throughout HRDC. From a non-technical perspective, a strong ITS awareness program is often viewed as the most important foundation from which to build an effective ITS program; ITS is everyone's responsibility. At the time of this audit, Business Continuity Plans were required for a few mission critical programs. HRDC also needs to review how passwords are used to access its systems; specifically the number of passwords that exist, policies that pertain to these passwords and technical solutions to alleviate some staff from having to remember multiple passwords for different systems.

For Phases II (OTVA) and III (ANST), AED collaborated with the Communications Security Establishment (CSE) to undertake a Security Posture Assessment (SPA) of HRDC to determine which systems and network vulnerabilities could be exploited. HRDC and CSE entered into a Memorandum of Understanding (MOU) which governed the conduct of the technical testing. In addition to the MOU, Ministerial Authorization was also obtained to conduct the SPA.

For Phase II, AED/CSE conducted an internal vulnerability assessment of HRDC's systems to assess the vulnerabilities of HRDC systems. The results of this assessment show the security inside HRDC's perimeter defenses provides opportunities for improvement. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. There is no comprehensive configuration management process and, as such, some regions are configured differently. Most internal traffic goes [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

For Phase III, AED/CSE conducted an external vulnerability assessment of HRDC's systems to assess the vulnerability to electronic attacks of HRDC's perimeter networks. The activities conducted simulated those to be expected of an internet threat agent (i.e. 'hacker') targeting HRDC's networks. The results of this assessment show the perimeter defenses of the HRDC systems that were tested to be sufficiently strong. However, other methods were found to exploit vulnerabilities within some HRDC systems resulting in a compromise of HRDC's internal network. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. As a result of this assessment, there are opportunities for HRDC to improve its security posture.

In conclusion, with the increasing complexity and frequency of attacks on computer systems, it is to be expected that an IT environment as large and diverse as HRDC's would have areas for improvement to enhance its ITS. With management's support, this audit was undertaken to identify these areas for HRDC to now priorize and address. While the audit's findings and recommendations can not guarantee that an unauthorized person or entity will not gain access to HRDC's systems and networks, they should assist HRDC in developing an overall ITS risk mitigation strategy and enhancing its ITS environment.

1.0 Introduction

1.1 Background

N.B. Subsequent to this audit's commencement, HRDC transformed into two departments, namely SDC & HRSDC, on December 12, 2003. This report refers to HRDC in the context of both SDC & HRSDC.

The objectives of this three-phased Comprehensive Audit of HRDC's (SDC & HRSDC) Information Technology Security (ITS) were to provide departmental senior management with an assessment regarding HRDC's:

1. ITS Governance Framework;
2. Internal ITS Vulnerabilities: On-Site Technical Vulnerability Assessment (OTVA); and
3. External ITS Vulnerabilities: Active Network Security Testing (ANST).

As approved by HRDC's Audit and Evaluation Committee (AEC), the audit's Objectives, Scope, Standards, and Methodology are in Appendix A.

ITS can be briefly defined as the control structure established to manage the integrity, confidentiality, and availability of IT data and resources. This control structure requires a management framework and governance structure. Phase I assessed HRDC's ITS management, operational, personnel and technical controls in relation to it's ITS Governance Framework.

Within the context of these controls, Phase I also followed up on the issues noted in two previous ITS audits. In September, 1999 HRDC's Internal Audit assessed the department's ITS, noting a need to streamline HRDC's organizational structure and processes to manage ITS at all levels and enhance the knowledge and awareness of all HRDC personnel regarding ITS. In April, 2002, the Office of the Auditor General's (OAG) ITS audit (which included HRDC) noted similar findings and stated that the Government Security Policy (GSP) requires a report on the effectiveness of ITS across government by 2004. This audit will assist the department to respond accordingly to this requirement. Lastly, Phase I documented HRDC systems (e.g. IP addresses) that were used for the technical testing in Phases II and III. For Phase II (OTVA), we conducted an internal vulnerability assessment of HRDC's systems to assess the vulnerabilities of HRDC systems/informational assets. For Phase III (ANST), we conducted an external vulnerability assessment of HRDC's systems to assess the vulnerability to electronic attacks of HRDC's perimeter networks.

In preparation for this audit, SDC's Audit and Evaluation Directorate (AED) consulted with representatives from the:

- OAG, IT Audit Services;
- Treasury Board of Canada, Secretariat (TBS) Government Operations Services;
- TBS, Chief Information Officer Branch;

- The Royal Canadian Mounted Police, Technical Security Branch; and
- Communications Security Establishment (CSE), who ultimately partnered with AED to collaboratively perform the technical testing for Phases II and III.

Fieldwork for Phase I was from October 2003 to March 2004, Phase II from February 2 to 16, 2004, and Phase III from March to September 2004.

2.0 Phase I Findings – ITS Governance Framework

2.1 Management Controls

2.1.1 ITS management structure has been documented, integrated into HRDC's programs, and supported by all levels of management

As per the TBS GSP, HRDC has designated a Departmental Security Officer (DSO), within the Finance and Administration (FAS) Branch, who establishes and directs a security program, including ITS. However, due to the technical nature of ITS, a Memorandum of Understanding (MOU) between FAS and the Systems Branch has been signed that delegates the ADM, Systems as accountable for ITS.

Within the Systems Branch, ITS responsibilities involve all four Systems Directorates.

- Policy, Strategic Management and Planning (e.g. policies, procedures)
- Technology Services (e.g. processes, governance, security engineering)
- IT Operations (e.g. computer centers – main frames, servers)
- Client Solutions (e.g. software development/standards)

Other departmental Branches (e.g. Employment Insurance (EI), Income Security Programs (ISP)) have been actively participating in identifying ITS security requirements through Privacy Impact Assessments (PIAs), Threat & Risk Assessments (TRAs), and maintaining systems access profiles levels that align job duties with access to appropriate information.

The department's Regional Headquarters (RHQ) and local offices have physical and IT security responsibilities within their organizations through their respective Regional Security Officers (RSOs), Local Area Network (LAN) staff and Program Managers.

Although the department has adequately documented, integrated and supports its ITS management structure, some issues were noted.

HRDC's 'Privacy Management Framework Steering Committee' (PMFSC) is a decision making committee that addresses privacy issues. Recent PMFSC minutes state that the PMFSC committee's mandate is being reviewed to include security responsibilities but nothing has occurred to date.

While we could not find a similar decision making committee for ITS issues, we did note the creation of the Information Technology Security Governance Committee (ITSGC), an ITS advisory committee that convened its first meeting on October 27, 2003. To date, no minutes from this inaugural meeting have been released. A second meeting was held on July 27, 2004.

Although ITS is referenced within corporate, Systems' and regional plans, we could not find an official departmental ITS strategy/vision document that these plans either emanated from or supported.

Recommendation No. 1: It is recommended that the Privacy Management Framework Steering Committee's mandate and name/title expand to include 'Security'.

Recommendation No. 2: It is recommended that the Information Technology Security Governance Committee:
a) produce a departmentally authorized ITS strategy/vision document;
b) create meeting minutes/records of decisions;
c) meet quarterly; and
d) report through the Privacy Management Framework Steering Committee.

2.1.2 Practical and useful ITS policies and procedures have been expeditiously disseminated to appropriate users

ITS policies and procedures are located on the departmental Intranet. Different sources, such as Systems, FAS, etc. have contributed to these policies and procedures that are supported and communicated by senior management for appropriate users. For example, Systems creates firewall policies and rules while FAS creates departmental ITS policies and procedures for Internet and e-mail usage.

While we have noted that the department has expeditiously disseminated ITS policies and procedures to appropriate users, some improvements could be made to address the following issues.

Some regions expressed confusion as to who is responsible to create and authorize ITS policy. The Systems/FAS MOU defines Systems, (i.e. Policy Strategic Management and Planning (PSMP) Directorate) as responsible for ITS policies. Within the Informatics Technology Security Services (ITSS) web site, under Policy, Processes and Governance, ITSS responsibilities have been identified to include "the identification of relevant policies, standards and guidelines", but not responsible to authorize them. The ITSGC can not authorize ITS policies as it is an advisory committee.

While ITS policies exist, our analysis indicated that they were not signed-off by senior management. Further, of the 30 ITS policies and procedures obtained from Systems and other websites, six were in 'DRAFT' status, one from 1999, one from 2000, two from 2001, and two unknown.

Recommendation No. 3: It is recommended that:
a) the department engage an appropriate governance structure (e.g. ITSGC, PMFSC, etc.) to authorize ITS policies; and
b) Systems submit 'DRAFT' ITS policies to the appropriate governance structure for authorization.

Regions are requesting national ITS procedures/guidelines to address issues/areas that they believe are still outstanding such as policies pertaining to access, mobility, etc. Since these types of specific ITS policies have not yet been nationally sanctioned, some regions have developed their own which can cause inconsistencies amongst regions. We, along with CSE, our technical testing partners for Phases II and III of this audit, have confirmed the variances amongst regions in their inconsistent configurations for desktops, Local Area Network Systems (LANs), and servers.

Recommendation No. 4: It is recommended that Systems, in conjunction with the regions, identify and develop required national ITS policies and procedures.

2.1.3 Risk management is a formal management process and has been integrated into System's management practices which includes ITS

Systems risk management sessions were scheduled and performed in 2003, which have identified Privacy/Security as a high risk. System Branch Profiles have been developed along with associated Risk Mitigating Strategies that are monitored.

The departments' four Information Technology Centers (ITCs) have recently performed TRAs. Along with these TRAs, formal risk management sessions have also been done by Systems. As mentioned above, departmental branches (e.g. Employment Insurance, Income Security Programs) are identifying ITS risks through PIAs and TRAs.

Some regions visited have implemented risk management processes, which subsequently have been inputted into their regional Operational Planning exercise. These included associated action plans, that have identified ITS as a major risk.

2.1.4 Formal ITS audits and reviews have been done and findings addressed in action plans

Formal ITS audits and reviews have been performed and associated action plans created. These audits and reviews have been performed by the department's Internal Audit, Systems' ITSS and ITC Operations as well as the OAG. TBS and OAG receive internal ITS related audit reports as both are members of the department's AEC, the forum at which departmental audits and reviews are tabled.

2.2 Operational Controls

2.2.1 ITS policies/procedures describe HRDC's ITS roles, responsibilities (R/Rs) and services

ITS policies/procedures describe roles and responsibilities through items such as the FAS/Systems MOU, departmental (i.e. national, regional, and local) LAN Administrator's job descriptions, and Regional Information Technology Security Liaison (RITSL) positions. ITS policies/procedures also describe a plethora of services such as the department's Firewall Policy, [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], HRDC IT Security and Privacy Co-Location Guidelines, Password Requirements, and Service Level Agreements (i.e. Ontario region).

2.2.2 ITS R/Rs and services have been assigned to appropriate people and groups, however, not all are appropriately resourced to fulfill their mandate

We have verified that the following ITS R/Rs are assigned to appropriate people and groups.
i) ITS training and awareness
ii) identification of IT assets
iii) security screening (including contracts)
iv) physical security/protection of employees
v) business continuity/resumption planning
vi) security incident investigations.

We have also verified that ITS R/Rs are clearly documented for:
i) DSO ITS functions
ii) Systems ITS functions
iii) System owners (e.g. EI, ISP, etc.)
iv) National, regional and local staff

Of the national and regional ITS representatives with whom we spoke, they expressed a general satisfaction that they are appropriately resourced to fulfill their mandate.

However, we did note one exception with the department's Information Protection Control (IPC) group. IPC has been recently formed to monitor, respond to and report against ITS-related issues, including viruses such as Nachi and Blaster that have 'infected' the department. In our opinion, the IPC's function is critical, however they do not yet have a plan indicating required resources to fulfill their mandate.

Reaction to managing these infections is both preventive and reactive. Preventive measures include software [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] that ensures anti-virus software is always on and confirms that configurations are secure (i.e. known vulnerable ports are closed). However, when new viruses (e.g. Sasser) do 'infect' the department, reactive measures include LAN Administrators having to physically visit each desktop to eradicate the virus.

Recommendation No. 5: It is recommended that Systems should develop a plan (including resources) for the Information Protection Control group.

2.2.3 ITS Business Impact Analysis (BIA), Threat & Risk Assessments (TRAs), Business Continuity Plans (BCPs), Disaster Recovery Plans (DRPs), and Emergency Response Plans (ERPs) are not all documented, current and tested

We observed that the FAS DSO office has collected BCPs for national program areas and regions. In addition to being documented, BCPs are current and tested in that they were updated and revised within the last year. We also noted examples of BCPs that were recently invoked and worked well. Also, the Systems' web site has the documented and current (FY 2002/03) BCPs for the four departmental ITCs. TRAs have also been recently performed (FY 2002/03) for all ITCs.

However, we noted that some recently implemented mission critical software/internet applications, in the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]; management is now taking action. Three of the four ITCs' BCPs have been fully tested. While the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] BCP conducted a simulation exercise in February, 2004 it remains to be fully (operationally) tested, with plans to do so in Q4 of 2004.

Recommendation No. 6: It is recommended that Systems should continue with expeditiously concluding Business Continuity Plan testing for:

a) all mission critical software applications in the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]; and
b) the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

As per the OAG's recommendation from its 2002 ITS audit to conduct a global TRA, an Enterprise Statement of Sensitivities (SoS), initiated by Systems' ITSS group, has been completed within the last year. This is the first stage in a more global TRA scheduled to be started this fiscal year (2004/05). Although TRAs have been performed for new and major changes to applications and infrastructure within the department, we could not find any departmental criteria or baseline to determine when a TRA should be initiated for major changes. Our discussions with representatives from departmental software application groups indicated that performing TRAs were frequently judgmental and arbitrary. In the absence of criteria and baselines on when to do a TRA, this could lead to TRAs not being performed when required.

Recommendation No. 7: It is recommended that Systems, in collaboration with the Departmental Security Officer, should identify specific criteria and baselines to determine when TRAs must be performed.

2.2.4 An effective Incident Response process exists

We noted that there was no formal definition of what constitutes an ITS Incident, however, IT incidences and problems are reported through the department's National Service Desk (NSD). The NSD forwards the problem to the appropriate 'Resolver Group' (which can include LAN Administrators, ITSS, DSO and IPC groups), by issuing 'trouble tickets', which the NSD records and tracks through to resolution. This includes hardware and software problems (including viruses). Sensitive incidences (e.g. internet abuse) are reported to the DSO/RSO for investigation and presented, if warranted, to the appropriate level (e.g. Supervisor, Human Resources, RCMP, etc.) for disciplinary action. As per the GSP requirement, we also noted that security incidents are collected and archived.

Recommendation No. 8: It is recommended that Systems, in collaboration with the Departmental Security Officer, clearly define what constitutes an ITS incident and communicate it to all staff.

2.2.5 ITS has not been appropriately considered throughout the department's System Development Life Cycle

The department's existing Project Life Cycle (PLC), posted on Systems' PLC web site, first identifies 'security' at the Design (3rd) phase. However, the OAG's 2002 ITS Audit Report recommended having ITS start at the Initiate (1st) phase which is in accord with Systems' ITSS web site. Also, ITSS has recently developed an ITS Model that identifies all ITS requirements at each of the PLC's six phases. While this Model has been presented and approved by Systems' General Management Committee, it has yet to be implemented and adopted into the systems PLC.

Recommendation No. 9: It is recommended that Systems should:
a) implement Information Technology Security (ITS) Services' ITS Model; and
b) update their Project Life Cycle web page to reflect the new ITS requirements.

The department has a Project Review Committee (PRC) whose "role is to contribute to a project's success by applying the best practices of gated reviews, risk assessment, and standardised project life cycle methodologies and tools"; this 'role' includes ITS requirements and deliverables (e.g. TRAs, DSO consultation, contracts, etc.). With the PRC not having met in over a year, it is our opinion that there is a risk some departmental projects may not be adhering to 'best practices' and compromising ITS requirements. For example, it is our understanding that some projects, such as [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], did not consider ITS requirements early enough in the PLC. This resulted in ITS requirements being reviewed and changed after contractual agreements with vendors had already been signed. Such 'after-the-fact' ITS practices could be costly to the department in a number of ways.

Recommendation No. 10: It is recommended that Systems should re-establish the Project Review Committee (or similar governance structure) to ensure ITS requirements are addressed.

2.3 Personnel Controls

2.3.1 A departmental ITS Awareness Program has not yet been nationally implemented

CSE representatives have indicated that one of the "biggest impacts" for ITS is awareness as it sets the tone and culture for security within an organization. ITSS convened an ITS Awareness Forum on March 24, 2004 with departmental representatives (including ITCs, regions and DSO) to discuss a phased-approach to nationally implement an ITS Awareness Program. ITSS has also posted a draft 'ITS Awareness Program' (May 2004) on their web page. Our analysis of this 'Program' indicates that it is both practical and thorough. We commend ITSS' initiative and support the ultimate implementation of a departmental ITS Awareness Program.

Recommendation No. 11: It is recommended that Systems should finalize and nationally implement a departmentally sanctioned Information Technology Security Awareness Program.

2.3.2 Personnel-related ITS policies/procedures (e.g. e-mails, appropriate computer usage, etc.) have been regularly communicated to staff

As previously indicated, many ITS policies and procedures exist, including personnel-related. These policies have been regularly communicated to staff, be it from the ADM, Systems through to LAN Administrators via e-mails, pop-up screens, corporate communications and web sites.

2.3.3 Security clearances are done for most personnel accessing the department's data including non-departmental personnel (e.g. provincial, other government officials, contractors) but issues were noted specific to security clearances expiring and provincial employees

All regions visited followed the GSP policy requirement that all employees, including students and contractors, need to have appropriate security clearance prior to commencing their duties. We received confirmation from the DSO that contractors used by the department have appropriate security clearances and observed examples of such being the case.

Security clearances have expiration dates depending upon the type of clearance (i.e. Secret expires after 10 years, Top Secret expires after 5 years, etc.). Per the GSP's security clearance process, the department has an 'Expiration of Security Clearances'

process that "updates reliability status and security clearances regularly". After analyzing the statistics for the expiration of security clearances, we conclude that all regions are adhering to the process reasonably well, [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

Recommendation No. 12: It is recommended that [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

We were informed by RHQ and NHQ staff (including the DSO) that [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], the GSP specifies that "departments must implement this policy (i.e. GSP) when sharing Government of Canada information and other assets with other governments (including foreign, provincial, territorial, and municipal), international, educational and private sector organizations….and departments must limit access to classified and protected information and other assets to those individuals who have a need to know the information and who have the appropriate security clearance level."

Recommendation No. 13: It is recommended that the Departmental Security Officer and Regional Security Officers should determine:

a) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]; and
b) if such is not the case, what remedial actions can be taken to address the situation.

We also analyzed all National Capital Region LAN Administrators security clearances and confirmed that they have the appropriate security clearances.

2.3.4 The department has ensured that all IT-related items are accounted for among present and departing staff

Hardware documentation/inventories are kept by the LAN Administrator. Software licenses, hardware inventory (on site and off site e.g. laptops, at home PCs), access to ITC mainframes are recorded and managed. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

Departing employees must complete a 'Separation Clearance Certificate - Form ADM 5017' to ensure that all 'IT Equipment' is accounted for. Further, this form must be signed by the departing employees' Responsibility Center Manager who forwards it to HR for final processing. However, the form does not specifically identify the termination of 'logical access' rights/methods, such as passwords, user codes, [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], etc., into departmental systems. Not terminating a departing employees 'logical access' leaves the department at risk of allowing a former employee to access departmental systems for which the employee no longer has the right or need to do so.

Recommendation No. 14: It is recommended that the department's 'Separation Clearance Certificate - Form ADM 5017' be revised to ensure that a departing employee's 'Logical Access' has been accounted for.

2.4 Technical Controls

2.4.1 ITS safeguards (e.g. firewalls, anti-virus) are being maintained, monitored (e.g. ITS attacks) and adjusted (as warranted) but improvements can be made

HRDC has taken steps to ensure ITS safeguards are being maintained, monitored and adjusted by securing the department's network through firewalls, ensuring anti virus software is current, implementing e-mail gateway filtering, controlled software distribution, authentication and encryption [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], etc. and monitoring external ITS attacks.

As mentioned in 2.2.2 above, the IPC group has been recently formed to monitor, respond to and report against ITS-related issues, including viruses. Also, the Infrastructure Vulnerability Emergency Response Team (IVERT) is a national, cross-sectional organization that is mobilized for emergency action against viruses within the department. The Anti Virus Project has implemented tools (e.g. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]) to prevent viruses from infecting the department. HRDC also uses [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] for desktop PCs and servers and new tools are being reviewed to further strengthen security within the department. We also noted that departmental officials review various information sources pertaining to ITS safeguards such as the Computer Emergency Response Team (CERT), Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), SANS Institute advisories as well as [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

While the above are good practices, we noted the following areas for improvement.

ITC's have recently purchased new data disks for the mainframe computers that run some of the department's major applications such as Employment Insurance and Canada Student Loans. As part of the purchase agreement for these disks, the vendor ([The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]) is to provide on-line technical support that includes monitoring and problem detection of these disks using software allowing for an automatic dial-up connection between the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

Recommendation No. 15: It is recommended that Systems should:

a) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
c) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]

Knowledgeable sources confided in us that [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

Recommendation No. 16: It is recommended that Systems should implement (and monitor adherence to) a policy/directive that states only departmentally authorized technology (e.g. servers) can connect to the departmental network.

During our local office visits, we noted some office cubicles, used by our service representatives to greet/interview clients, have departmental desktop computers placed on the employees' desks in such a way that allows clients access to the back of these computers. Allowing clients physical access to an employee's unsecured computer could result in the destruction of government property as well as risk having clients access the ports at the back of the PC, which may compromise security. Some of the regions we visited recognized this issue and took steps to secure such computers, thus restricting clients' access to them.

Recommendation No. 17: It is recommended that Systems should implement a policy/directive requiring all staff computers be protected and secured from public/client access.

Industry standards indicate that regular internal and external penetration testing of an organization's IT systems should be done, as is stated in the ITSS mandate. Although we noted that internal penetration testing is done ad hoc, we could not find a plan/schedule for regular internal and external penetration testing on the network.

Recommendation No. 18: It is recommended that Systems conduct regular internal and external penetration testing on the departmental network.

2.4.2 Logical access controls have been be implemented but improvements can be made

Logical access controls within this department are determined by the hardware and software implemented (i.e. platform dependent). Both mainframe and server environments, such as [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], etc., actively control logical access through user codes, passwords, access control lists, profiles and other methods. A draft usercode password policy has been developed.

We noted that although the department has implemented logical access controls, improvements can be made as we indicate below.

To date, within the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], we could not find evidence of any departmental assessments having been done to ensure conformance to the government standard for passwords of 8 alpha numeric characters that are changed every 90 days. We (in collaboration with CSE) discovered that almost half (49%) of the 34,891 passwords we reviewed were less than 8 characters. [The information withheld qualifies

for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. Presently, the department has neither an authorized departmental policy nor implemented a technical solution to ensure that the government standard for passwords is enforced.

Recommendation No. 19: It is recommended that Systems should implement a policy and technical solution to ensure the government standard for passwords is enforced.

Some regional office employees work with many different applications (e.g. I&C, EI, NESS, CMS, etc.) operating on different platforms (e.g. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], etc.), each requiring unique usercode passwords. We were informed that an employee could have up to 12 work-related user code passwords making it difficult to remember all of them. We were told that employees often write down their usercode password and 'hide' it under their keyboard, computer, telephone, in their desk drawers, etc. We were also told that employees often select the same usercode password for different applications and select easy to guess usercode passwords. As a result, HRDC's usercode password environment [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. The Security Management Single Log On (SMSL) project was to address some of these concerns. However, this project has not progressed as planned due to funding restraints. While the implementation of a usercode password policy and technical solution to ensure government standards are maintained would be beneficial (Recommendation No. 19 above), it still does not address the issue of some staff requiring numerous usercode passwords and how they 'hide' them.

Recommendation No. 20: It is recommended that Systems should implement a technical solution that reduces the number of usercode passwords some employees require to access multiple systems.

As part of the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] mainframe security administration, a security software package, called [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], produces a paper report identifying all users who access the various mainframes systems. This report is sent on a regular basis from the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] representatives to the department's respective Responsibility Center (RC) managers for the latter to review and update it (if required) to reflect its accuracy (e.g. confirm, delete, add, modify, etc. users' access to the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] mainframe). However, RC managers presently do not have to send the results of their review back to the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]; there is no requirement for the RC managers to acknowledge if the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] report accurately reflects their access requirements. Our analysis of the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] report with some RC recipients indicated RC users who still had valid access to mainframe systems when such should not have been the case.

Recommendation No. 21: It is recommended that Responsibility Center managers should ensure that their [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] reports are actioned within two weeks of their receipt and promptly returned to the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

The printing and distribution of [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] reports from the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] to the departmental RCs is a manual process that appears to be conducive to the economies and efficiencies of a web application.

Recommendation No. 22: It is recommended that Systems should explore the feasibility of publishing the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] reports on a website.

2.4.3 Access to computer/server rooms are controlled

All computer/server rooms we observed were restricted to authorized individuals through card and key access, equipped with alarms and could produce reports that identified access. However, one concern we have is the large number of people accessing some of the regional [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] we visited. The department has [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] that consolidate enterprise-wide servers to better support the national infrastructure. The architecture uses a regional model whereby each region has one or more dedicated [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] to provide business services. In light of our concern, the regions we visited are now reviewing [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] access.

Recommendation No. 23: It is recommended that Systems and regions should restrict access to their [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] to only those requiring it.

2.4.4 Data back-ups regularly occur

All [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] and [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] visited are performing data backups regularly and storing them off site.

2.4.5 HRDC are not employing metrics to assess the effectiveness of ITS

Although various IT reports (e.g. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], etc.) are available,

tracking trends and monitoring activities is often done in an ad-hoc manner. However, specific to ITS, we could not find any formal process of metrics, such as Key Performance Indicators, that are analyzed against pre-determined standards or criteria to assess the effectiveness of ITS.

Recommendation No. 24: It is recommended that Systems should develop metrics to assess the effectiveness of ITS.

2.5 Status: Previous Audit Findings

2.5.1 IARMS, September 1999

In section 2.1.4 above, we acknowledge that "formal ITS audits and reviews have been done and findings addressed in action plans" as action plans were developed with good intent based upon the information at that time. However, based upon our audit work above, we also noted that some action plans did not always work out as originally envisioned.

In September 1999, we conducted an audit of HRDC's ITS, noting a need to:

- streamline HRDC's organizational structure and processes to manage ITS at all levels;
- enhance the knowledge and awareness of all HRDC personnel regarding ITS.

Based upon our audit findings above, we conclude that, while progress has been made on streamlining HRDC's organizational structure and processes to manage ITS, there are still areas for improvement. While we note in section 2.2.2 that ITS roles and responsibilities have been documented and assigned, they are still somewhat fragmented in that they do not always work in a unified and seamless manner to maximize ITS synergies. As we note in section 2.1.1 above, we believe further improvements can be made to develop a more cohesive ITS governance structure, however progress has been made (e.g. ITSGC). Lastly, we also note in sections 2.3.1 and 2.3.2 that progress has been made on enhancing the awareness and knowledge of all HRDC personnel regarding ITS and developing a DRAFT departmental ITS Awareness Program (and recommend national implementation of this program).

2.5.2 OAG, April 2002

In April 2002, the OAG conducted an audit of HRDC's ITS, noting much the same things we did in our 1999 audit, such as the need to:

- better implement the ITS governance framework *(Sections 2.1.1 and 2.1.2)*;
- conduct broad-based risk assessments *(Section 2.1.3)*;
- provide employees with adequate training in ITS awareness *(Sections 2.3.1 & 2.3.2)*;
- ensure that ITS is considered at the start of a system development life cycle *(Section 2.2.5)*;
- carry out ITS audits/reviews - including technical vulnerability testing *(Section 2.1.4)*;
- address other issues *(Section 2.0 - Findings)*.

In essence, our elaboration in section 2.5.1 above is also applicable to what the OAG noted. We also indicate *(in parenthesis)* the sections in this current report where we more specifically comment on what the OAG noted.

Additionally, the OAG employed the services of Electronic Warfare Associates (EWA) to conduct technical (vulnerability) tests within HRDC during their April 2002 ITS audit. To follow up on the status of the OAG's (i.e. EWA's) test results, we, in turn, also employed EWA for this current audit. EWA concluded that "Overall, HRDC responded appropriately to the internet vulnerabilities identified in the OAG Audit Report…(and) adequately addressed the items identified during the OAG Telephony VA".

3.0 Phase II Findings – Internal ITS Vulnerabilities (On-Site Technical Vulnerability assessment – OTVA)

3.1 Introduction

AED, in collaboration with the CSE, conducted an internal vulnerability assessment (i.e. OTVA) of HRDC's systems in order to provide an assessment of the vulnerabilities of HRDC systems/informational assets. The OTVA was conducted from February 2 to 16, 2004.

The OTVA exercises consisted of:

- Network Discovery and Vulnerability Assessment
- Firewall Rules Assessment
- Password Assessment
- 802.11b/a Wireless LAN Discovery
- Mobile Device Policy Review

3.2 Findings and Recommendations

The results of this assessment show the security posture inside HRDC's perimeter defenses provides opportunities for improvement. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. Many operating systems and applications [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. There is no comprehensive configuration management process and as such, different regions are configured differently. Most internal traffic goes through [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. A high percentage of threats are internal, these vulnerabilities should be considered priority items.

HRDC should review, prioritize, and resolve the above issues based on a Threat and Risk model. For example, some of the systems assessed have vulnerabilities that fall [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] and should be considered priority items.

A summary of recommendations for each of the OTVA activities follows.

- Network Discovery and Vulnerability Assessment
  - [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
  - [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]

- Maintain an up to date list of hosts connected to HRDC's networks.
- Ensure services are protected adequately by passwords.
- Perform network discovery, port scans and vulnerabilities assessments on a regular basis.
- [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
- Reinforce the naming convention of the system names to prevent the revealing of their network functions for an unauthorized user.
- [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
- Harden the software installations.
- [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]

- Firewall Rules Assessment
  - Review and update the firewall policy.
  - Review the traffic rules for support personnel and ensure that an appropriate change management procedure is in place in order to maintain a current and accurate list.
  - Recommend a screening or filtering router be used to block access to unused services on any of the untrusted interfaces on the firewalls.
  - Implement an addition to the service provider's filtering routers, its own screening routers; which can be monitored and occasionally reviewed or that a process be implemented whereby HRDC can audit the security features and Access Control Lists (ACLs) of the Service Provider's filtering routers.
- Password Assessment
  - Enforce and update the password policy to ensure strong password selection.
  - Perform a regular password assessment on other network zones and systems to ensure compliance to the password policy.
  - Remove the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] from every system if they are not used.
  - Keep the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] accounts i.e. system accounts with no password (NP) because these accounts should not be accessible from the network and should have limited or no privileges.
- 802.11b/a Wireless LAN Discovery
  - [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
  - [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
  - [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
  - Put in place a VPN or secure WLAN [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
  - Create and enforce a policy that governing wireless networks.
  - Perform regular discovery audits to determine whether new unauthorized access points have been installed.

- Mobile Device Policy Review
  - [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
  - Use a VPN with CSE approved cryptography and a personal firewall for Internet connectivity.
  - Update the policy to address the issues of software installation by users, surfing the Internet for private use, updating software with the latest patch and service pack, etc.

4.0 Phase III Findings – External ITS Vulnerabilities (Active Network Security Testing – ANST)

4.1 Introduction

AED, in collaboration with the CSE, conducted an external vulnerability assessment (i.e. ANST) of HRDC's systems in order to provide a risk evaluation of the vulnerability to electronic attacks on HRDC's perimeter networks and test the incident response and handling capabilities of HRDC to electronic attacks. The ANST was conducted from March 8 to September 1, 2004.

The ANST exercises consisted of:

- Network Scanning and Probing
- Probing of Wireless Devices
- Probing of Public Switched Telephone Network (PSTN)-Connected Modems
- Social Engineering Attack
- Exploitation of Vulnerabilities on Internal Hosts
- Password Cracking and Password Re-Use
- Detection of ANST activities
- Clean up

4.2 Findings and Recommendations

The ANST team conducted the activities expected of an Internet threat agent targeting HRDC's networks. Although the activities performed demonstrated that the perimeter defences of systems are sufficiently strong, exploiting vulnerabilities in the higher layer protocols compromised the internal network. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].

[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. As a result of this assessment, there are opportunities for HRDC to improve its security posture.

The following recommendations are provided for HRDC consideration, in order to increase the security posture of its networks and to reduce the likelihood that unauthorized individuals could gain access into these networks.

- Continue to secure perimeter devices
- [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
- [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]

- Review and enforce password policy
  - Replace password authentication mechanisms with two-factor mechanisms for all sensitive network services.
  - Develop a user-awareness program that includes instructions aimed at reducing password reuse.
- Encrypt sensitive web application traffic
  - [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]
- Deploy internal firewall
  - The internal network should be protected by internal firewalls that limit the type of traffic to those that are authorized by a network security policy.
  - Provide system log to detect intrusions or internal scanning and probing activities.
- Develop User-Awareness security program
  - Provide points of contact for reporting problems and on how to handle unsolicited e-mails, as well as e-mails containing e.g. block password protected Zip files and other dangerous file types through e-mail.
- Disable unnecessary internal services
- Deploy intrusion detection system within the internal networks
  - Combined with the internal firewalls, the use of intrusion detection systems within the HRDC's internal networks can impair an attacker's ability to extensively compromise the internal networks.
- Baseline and monitor traffic at egress point
- Remove unnecessary banner information
  - Limit to provide the information for external services in order to reduce the amount of information useful to an attacker through the Internet.

Appendix A

Objective, Scope, Standards & Methodology

Objectives

Phase I - HRDC's ITS Governance Framework

The Phase I objectives will assess HRDC's ITS controls, follow up on issues noted in two previous ITS audits of HRDC, and document a network map of HRDC systems that will be used for the technical testing in Phases II and III.

HRDC's ITS Governance Framework will be assessed against the following four ITS control principles, which incorporate the primary elements of the TBS-GOS' GSP, TBS-CIOB's MITSS, RCMP's TSSIT and ISO/IEC 17799 ITS standard. These ITS control principles adhere to and support the Information Systems Audit and Control Association's (ISACA) internationally-recognized Control Objectives for Information and related Technology standards.

a) Management Controls
b) Operational Controls
c) Personnel Controls
d) Technical Controls

Phase I will assess HRDC's status in addressing the issues raised in two previous ITS audit reports, one by the OAG (April 2002) and the other by IARMS (September 1999).

Lastly, IARMS will also document a network map of HRDC systems that will be used as the basis to conduct the technical testing for Phases II and III.

Phase II - Internal ITS Vulnerabilities: On-Site Technical Vulnerability Assessment (OTVA)

The Phase II objectives will be to conduct an internal vulnerability assessment of HRDC's systems in order to provide an assessment of the vulnerabilities of HRDC systems/informational assets.

Phase III - External ITS Vulnerabilities: Active Network Security Testing (ANST)

The Phase III objectives will be to conduct an external vulnerability assessment of HRDC's systems in order to provide a risk evaluation of the vulnerability to electronic attacks of HRDC's perimeter networks and test the incident response and handling capabilities of HRDC to electronic attacks.

Where required, IARMS will formulate recommendations for improving HRDC's ITS Governance Framework as well as its internal and external network security.

Scope

The 'Comprehensive Audit of HRDC's IT Security' will assess both non-technical (Governance Framework) and technical (Internal & External Assessments) elements. HRDC's NHQ [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] and the Quebec, Ontario, Alberta/NWT/Nunavut, and BC/Yukon regions will be visited during the conduct of the Audit. In consultation with select HRDC officials involved with IT Security, the systems for testing will be determined and resulting 'target lists' developed for the respective network diagrams, operating systems, IP addresses, phone numbers, wireless LANs, cell phones, PDAs and other wireless devices using the IEEE 802.11b wireless protocol.

Standards

The following audit standards are referenced from ISACA's COBIT standards which are an internationally-recognized IT/IM standard that is endorsed by other internationally-recognized IT entities such as IBM's PricewaterhouseCoopers Consultants and The Gartner Group.

Phase I: Standards – HRDC's ITS Governance Framework

a) Management Controls
- ITS management structure should be documented, integrated into HRDC's programs, and supported by all levels of management.
- Practical and useful ITS policies and procedures should be expeditiously disseminated to appropriate users.
- Risk management should be a formal ITS management process that is integrated into HRDC's management practices.
- Formal ITS audits and reviews should be done and findings addresses in action plans.

b) Operational Controls
- ITS policies/procedures should describe HRDC's ITS roles, responsibilities (R/Rs) and services.
- ITS R/Rs and services should be assigned to appropriate people/groups that are appropriately resourced to fulfill their mandate.
- ITS Business Impact Analysis (BIA), Threat & Risk Assessments (TRAs), Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and Emergency Response Plans (ERP) are documented, current and tested.
- An effective Incident Response process should exist.
- ITS is appropriately considered throughout HRDC's System Development Life Cycle.

c) Personnel Controls
- An HRDC ITS Awareness Program should be nationally implemented.
- Personnel-related ITS policies/procedures (e.g. passwords, appropriate computer usage, etc.) are communicated to staff.

- Security clearances should be done for all personnel accessing HRDC data including non-HRDC personnel (e.g. other government officials, contractors).
- HRDC should ensure that all IT-related items are accounted for amongst present and departing staff.

d) Technical Controls
- ITS safeguards (e.g. firewalls, anti-virus) should be maintained (where appropriate), monitored (e.g. ITS attacks) and adjusted (as warranted).
- Logical access controls should be implemented.
- Access to computer/server rooms should be controlled.
- Data back-ups should regularly occur.
- HRDC should employ metrics to assess the effectiveness of its ITS.

IARMS envisions that using the above standards to assess HRDC's ITS Governance Framework will simultaneously allow IARMS to follow up on HRDC's status in addressing the following issues raised in two previous ITS audits.

OAG – ITS (Chapter 3, April 2002) noted a need to:
- better implement the ITS governance framework;
- conduct broad-based risk assessments;
- provide employees with adequate training in ITS awareness;
- ensure that ITS is considered at the start of a system development life cycle;
- carry out ITS audits/reviews (including technical vulnerability testing); and
- address other issues.

IARMS – Assessment of ITS (September 1999) noted a need to:
- streamline HRDC's organizational structure and processes to manage ITS at all levels; and
- enhance the knowledge and awareness of all HRDC personnel regarding ITS.

IARMS will develop a network map of HRDC's systems that will identify firewalls, routers, switches, hubs, application servers, other critical network components including subnet and IP address information for each of the network devices. This Map will be used to define the devices that will be part of the scope for Phases II and III.

The standards used for the technical testing in Phases II and III are traditional methods and activities that are frequently used by 'Threat Agents' (e.g. 'hackers', viruses, etc.) to compromise a system. Following is a brief overview of the standards that will be used to assist HRDC in identifying any existing/potential vulnerabilities.

Phase II: Standards – Internal ITS Vulnerabilities: On-Site Technical Vulnerability Assessment

a) Network/Host Scanning
- Discover the active devices on HRDC's network as well as other services (e.g. TCP, UDP, etc.) that are listening through the network discovery process.

b) Network Vulnerability Scanning
- Scan the active devices, identified in the network discovery process, for vulnerabilities using a network vulnerability scanner.

c) Router Assessment
- Examine selected router configuration files for secure configuration and operation.

d) LAN Switch Analysis
- Assess HRDC's switch implementation by focus on the security of the switch itself and analyzing the switch's ability to protect the network.

e) Wireless Access Point Discovery
- Identify IEEE 802.11b wireless LAN access points within HRDC's premises, using IEEE 802.11b wireless access point discovery tools.

f) Mobile Device Policy Review
- Assess the level of compliance of HRDCs mobile device policies/procedures.

g) Password Assessment
- Assess the password policy that is enforced on HRDC's systems using password auditing and recovery tools.

h) Dial-Up Discovery/War Dialing
- Search for unsecured and/or unauthorized modems, fax machines and other devices within a set range of phone numbers.

Phase III: External ITS Vulnerabilities: Active Network Security Testing (ANST)

a) Network Scanning
- Map HRDC's perimeter network by scanning network devices and war dialing (to demonstrate how a 'Threat Agent' could map HRDC's networks without HRDC detecting the activity).

b) Network Probing
- Probe HRDC's networks and computers to determine operating systems and the services offered on each of the found devices (to demonstrate how a 'Threat Agent' could do the same without being detected).

c) Vulnerability Identification
- Research the possible vulnerabilities associated with HRDC's network devices, services and operating systems.

d) Exploitation Research and Development
- Identify exploitable vulnerabilities (which allow safeguards to be bypassed and gain access normally not allowed) including wireless networks and devices.

e) Exploit Activities
- Determine degree of exploits by conducting some and/or all of the following activities.
  - Upgrade Access to Administrator/Root
  - Install a Backdoor
  - Install a Network Sniffer
  - Examine Network Device for Critical Information
  - Use Network device as a 'Jump Point'
  - Upload Marker File

Methodology

As per Treasury Board's Internal Audit Guidelines, assurance will be provided through interviews with national, region and local office staff who are either involved with or impacted by ITS. Documentation reviews and sampling (e.g. ITS policies/procedures, firewall logs, TRAs, security clearances, Incident Response Reports, etc.) will be undertaken.

IARMS plans to conduct this audit as follows.
Phase I – Q3 (03/04), Phase II – Q4 (03/04), Phase III – Q1 (04/05).

IARMS will work in close collaboration with Systems to ensure appropriate safeguards are in place for the internal and external vulnerability assessments.

Appendix B

Management Action Plans

* Denotes a measure which will be implemented based on availability of funding. Should funding not become available, alternative strategies are being developed.

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
Phase I			
Recommendation No. 1: It is recommended that the Privacy Management Framework Steering Committee's (PMFSC) mandate and name/title expand to include 'Security'.	At June POC presentation, security was included as part of the PMFSC responsibilities. Policy and Modern Management Directorate (PSMP) is investigating whether security will be officially incorporated into Privacy Management Framework mandate. Nada Semaan will bring to next meeting of PMFSC. Further, Systems Branch is currently undertaking a complete review of all governance structures, including those internal to the Branch, as well as ensuring linkages to departmental governance structures.	March 31, 2005	Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
Recommendation No. 2: It is recommended that the Information Technology Security Governance Committee (ITSGC): a) produce a departmentally authorized ITS strategy/ vision document; b) create meeting minutes/ records of decisions; c) meet quarterly; and d) report through the PMFSC.	a) - d) Meeting agendas and minutes are available for review by any party within the Departments. Meetings are called at the request of the co-chairs or recoding secretary and occur at least quarterly. Decision making and reporting structures are currently under review by TSD Management and will be made available once concluded and the reporting process and structures are settled. Architecture and Engineering will cooperate in the development of strategy & vision documents. Further, Systems Branch is currently undertaking a complete review of all governance structures, including those internal to the Branch, as well as ensuring linkages to departmental governance structures.	March 2005	Sr DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
Recommendation No. 3: It is recommended that: a) the department engage an appropriate governance structure (e.g. ITSGC, PMFSC, etc.) to authorize ITS policies; and b) Systems submit 'DRAFT' ITS policies to the appropriate governance structure for authorization.	a) - b) Systems Branch is currently reviewing the governance structures, including the ITSGC, and is working toward defining the policy instrument approval process to ensure the proper authorities are exercised in the approval of various levels of policy instruments. Currently, several "Draft" policies have been developed. Measures are being taken to refine and update these policies as appropriate. Each of these draft policies will be introduced into the approval process.	March 2005	Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 and Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
Recommendation No. 4: It is recommended that Systems, in conjunction with the regions, identify and develop required national ITS policies and procedures.	Systems Branch is moving forward with a comprehensive National IT Policy Framework that identifies IT Security policies as a foundational element for all Systems Branch activities. This covers the SDC National structure, which includes the Regions. An ITS Policy and Framework: IT Policy, was presented at SEMC and GMC in October 2004.	March 2005	Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 and Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
Recommendation No. 5: It is recommended that Systems should develop a plan (including resources) for the Information Protection Center group.	The IPC (Infrastructure Protection Centre) was established in October 2003 to lead NHQ/Operations' activity for PC virus troubleshooting nation-wide. It is comprised exclusively of resources from NHQ; however, it relies heavily on the collaboration of regional resources to actually remedy virus outbreaks when they occur. With one year's experience under our belt, NHQ recognizes the need to review the IPC function, - in terms of its duties, tool set, and resource levels to manage safe computing on the SDC/HRSDC network. From experience to date, we realize that closer association with NHQ and regional resources is tantamount to effectively managing safe computing on the SDC/HRSDC network. To that end, the IPC will take the lead to develop a plan of action to address this issue, cooperating and collaborating with the Regional IT security groups in the final quarter of the current fiscal year.	Q4 - 2004-2005	Sr. DG, Operations - Dave Holdham 934-0341 Mike Snider 997-8118

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
*** Recommendation No. 6**: It is recommended that Systems should continue with expeditiously concluding Business Continuity Plan testing for: a) all mission critical software applications [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]; and b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].	There were some BCP exercises performed this fiscal year and additional ones are being prepared: a) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. Additional servers are scheduled to be delivered before the end of this fiscal. Two exercises are planned this year: a paper exercise in November and a full recovery next Spring. b) A full BCP exercise was performed between [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] in May 2004 to [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. This exercise was a success. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	Spring 2005	Sr. DG, Operations - Dave Holdham 934-0341 Réjean Poitras 994-4183 Sr. DG, Operations - Dave Holdham 934-0341 Réjean Poitras 994-4183
Recommendation No. 7: It is recommended that Systems, in collaboration with the Departmental Security Officer, should identify specific criteria and baselines to determine when TRAs must be performed.	ITSS will collaborate with the Departmental Security Officer to develop TRA criteria and baselines, and incorporate them into the IT Security Process Model.	March 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
Recommendation No. 8: It is recommended that Systems, in collaboration with the Departmental Security Officer, clearly define what constitutes an ITS incident and communicate it to all staff.	NTS is represented at the ITSGC. Guidelines on Conducting Administrative Investigations have been developed which include ITS incidents. Human Resources have communicated these Guidelines to all regions. ITSS will develop sample definitions and put them forward for review and approval by the ITSGC; however it is felt that standard Government of Canada definitions should be forthcoming from Treasury Board.	March 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, Operations - Dave Holdham 934-0341 Mike Snider 997-8118 and DSO - FAS André Lefebvre 9971935
Recommendation No. 9: It is recommended that Systems should: a) implement Information Technology Security (ITS) Services' ITS Model; b) update their Project Life Cycle web page to reflect the new ITS requirements.	a) IT Security is in the process of integrating the Security (ITSS) Services' ITS Model in the SDLC/PLC. b) The Systems Project Management Office are referencing the IT Security process in updates to the Project Life Cycle.	Ongoing Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 Sr. DG, PSMP - Nada Semaan 997-1620 P. Charlsworth 953-3159
Recommendation No. 10: It is recommended that Systems should re-establish the Project Review Committee (or similar governance structure) to ensure ITS requirements are addressed.	The PRC framework has been presented and approved at SEMC and GMC. The first meeting was held in October 2004.	October 2004	ADM, Systems - Serge Rainville 997-6481 Ron Ramsey 997-8037
*** Recommendation No. 11**: It is recommended that Systems should finalize and nationally implement a departmentally sanctioned Information Technology Security Awareness Program.	ITSS is currently in consultations with national and regional subject matter experts, in cooperation with IPC and the regions, as we design and begin to implement a Security Awareness program for a variety of audiences suitable to an organization the size of SDC/HRSDC. Note: SDC no longer has a Regional structure now that the Regions report in to National Systems.	March 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 ADM, Systems - Serge Rainville 997-6481 Ron Ramsey 997-8037

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
Recommendation No. 12: It is recommended that the Departmental Security Officer and Ontario's Regional Security Officer should update security clearances within the Ontario region.	Regional Security maintains the security clearances of its employees. The Departmental Security Officer, on advice from regional security officers has the final authority in granting, revoking or denying a reliability status. Reliability status process requires a criminal record check conducted by the RCMP (police force of choice identified by TBS). In cases where a positive identification of the (candidate) employee is required by the RCMP, fingerprints are obtained and processed by the police agency. At present time, the RCMP is experiencing a processing delay of 180 days. Senior management has been informed of this situation and are kept informed of any changes in the RCMP processing timelines.	Completed	DSO - FAS André Lefebvre 997-1935
Recommendation No. 13: It is recommended that the Departmental Security Officer and Regional Security Officers should determine: a) whether provincial employees who access departmental (i.e. Government of Canada) information have appropriate security clearances; and b) if such is not the case, what remedial actions can be taken to address the situation.	a) - b) Provincial governments do not have a security clearance system for their employees. In centers where we have co-locations with provincial government employees, federal employees are regularly reminded to exercise appropriate safeguards in regards to protected and classified information. Such safeguards include not sharing protected or classified information held in federal data banks and ensuring that such documents are stored and manipulated according to departmental and TBS policy. This matter has been discussed at the department's Integrity Working Group Committee and brought to the attention of senior management.	Completed	DSO - FAS André Lefebvre 997-1935

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
Recommendation No. 14: It is recommended that the department's 'Separation Clearance Certificate - Form ADM 5017' be revised to ensure that a departing employee's 'Logical Access' has been accounted for.	The Separation Clearance Certificate form will be modified to incorporate the termination of access to departmental systems.	End of FY 2004-05	DSO - FAS André Lefebvre 997-1935
Recommendation No. 15: It is recommended that Systems should: a) verify [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], it is recommended that Systems should: b) implement audit trails to monitor [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] once inside the system; and ensure [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] who access client data have appropriate security clearances.	a) and b) Systems has verified that there is no means [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. It is technically impossible; therefore audit trails are not required	Completed	Sr. DG, TSD - Dave Adamson 956-5487 Pierre Lafrance 953-0702

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
Recommendation No. 16: It is recommended that Systems should implement (and monitor adherence to) a policy/directive that states only departmentally authorized technology (e.g. servers) can connect to the departmental network. **Same as Recommendation No. 1(c) - Phase II - Subset of Recommendation No. 4**	Currently there are policies in place on Network Usage. Further, as part of the Branch's policy renewal initiatives, all policies will be reviewed to ensure that monitoring plans are in place to support those policies. All future policies are to include monitoring plans.	March 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
Recommendation No. 17: It is recommended that Systems should implement a policy/directive requiring all staff computers be protected and secure from general public access.	Systems agrees with this recommendation and will ensure that this issue is addressed in the updated high-level departmental IT Security Policy instrument. A draft document is expected to be developed by the end of this fiscal year.	March 2005	Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 and Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
Recommendation No. 18: It is recommended that Systems conduct regular internal and external penetration testing on the departmental network.	ITSS conducts testing on an ongoing basis of new and existing systems as a part of the Vulnerability Assessment process using internal and external consulting resources to ensure the highest quality process are in place using the most modern and advanced tools and programs.	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act*.]	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
*** Recommendation No. 19**: It is recommended that Systems should implement a policy and technical solution to ensure the government standard for passwords is enforced.	Currently the Password policy is under review by the ITSGC and will be further supported with the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].	March 2006	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
Recommendation No. 20: It is recommended that Systems should implement a technical solution that reduces the number of usercode passwords some employees require to access multiple systems.	Currently there is a project that is proposed to put in place a process of designing and implementing [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] that will satisfy this recommendation. (Same product as Recommendation No. 19) • [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] • ITO will work in conjunction with A&E to implement Phase II once the project is funded and engineered.	March 2006 Phase I Completed	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and René Lalande 997-8693
Recommendation No. 21: It is recommended that Responsibility Center managers should ensure that their [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] are actioned within two weeks of their receipt and promptly returned to the ITCs.	The Systems branch agrees with this recommendation and will augment its effort to carry out regular follow up with the ITCs to ensure timely completion.	Ongoing	Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
Recommendation No. 22: It is recommended that Systems should explore the feasibility of publishing [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] on a website.	Systems will explore the feasibility of distributing the [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. The target date to get the feasibility study completed is April 2005.	April 2005 (study)	Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115 and René Lalande 997-8693
Recommendation No. 23: It is recommended that Systems and regions should restrict access to their Solution Centers to only those requiring it.	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	Completed	ADM, Systems - Serge Rainville 997-6481 Ron Ramsey 997-8037 and Sr. DG, Operations - Dave Holdham 934-0341 R. Poitras 994-4183
Recommendation No. 24: It is recommended that Systems should develop metrics to assess the effectiveness of ITS.	Systems supports this recommendation and will design metrics in support of the ITS process. (TBS self assessment tool to measure compliance.)	September 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
Phase II			
It is recommended that:			
1(a) all of the Operating Systems (OS), hosts, and servers that do not have the latest 'Service Packs/Security Patches' installed should be updated *(Network & Service Discovery, and Network Based Vulnerability Assessment)*;	1(a) Systems has an on-going activity to identify and patch all network connected devices. Given the critical service delivery nature of some of the hosted applications, some patches require extensive testing prior to implementation in the production environment. The fact that many of these hosts are located in protected network segments mitigates the risk of delaying the implementation of patches and service packs.	1(a) Completed	Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
1(b) the hosts/servers that were not included in the scan [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] should also be assessed and updated, if required (*Network Based Vulnerability Assessment)*;	1(b) Although the audit report does not single out specific hosts or servers that were not included in the scan; all systems should be scanned on a regular basis.	1(b) Completed	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
1(c) the hosts/servers [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] should be assessed in order to establish the requirement to maintain this [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Network & Service Discovery, and Network Based Vulnerability Assessment)*; **Same as Recommendation No. 16 - Phase I**	1(c) Systems intends [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] as part of its normal course of business. There is a plan in place to inventory and analyze existing hardware and [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] Servers. An upgrade path has been determined where possible and much analysis is required for the third party software running on these servers. Unfortunately, no funding has been allocated to this project to date.	1(c) Completed	Sr. DG, Operations - Dave Holdham 934-0341 René Lalande 997-8693

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
1(d) software installations should be hardened to improve the security of the network (*Network Based Vulnerability Assessment*); **Same as Recommendation No. 2(c) Phase II - below**	1(d) This recommendation clearly speaks to both platform and application hardening. Installation processes are in place that apply various hardening elements to all server builds. The CIR process for server builds encompasses many elements that are currently recommended [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*], industry best practices and Lead Agencies. Hardening standards are established by the responsible OPI and are applied universally unless exemptions are granted by order of management.	1(d) Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 René Lalande 997-8693 and Sr. DG, Client Solutions - Ron Meighan 994-0749
1(e) the naming convention policies should be reinforced to prevent involuntary divulgation of what could be an interesting target for an unauthorized user *(Network & Service Discovery)*; **Same as Recommendation No. 2(c) in Phase II**	1(e) Systems fully supports the implementation of a non-descript naming convention for all exposed assets on either internal or external networks. Systems will ensure that this issue is addressed in the updated high-level departmental IT Security Policy instrument. A draft document is expected to be developed by the end of this fiscal year.	1(e) policy issue: March 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733 and Sr. DG, Client Solutions - Ron Meighan 994-0749

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
1(f) regular network discovery and service scans should be performed to ensure the proper configuration of HRDC's networks, hosts, and services *(Network & Service Discovery)*;	1(f) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	1(f) Ongoing [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]: Q4 – assuming platforms are ready for use.	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115 and Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579
1(g) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Network & Service Discovery)*; and	1(g) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] by end of fiscal year and will continually coordinate with Regional Level 2 support groups.	1(g) March 2005	Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115
1(h) vulnerability assessments should be performed on a regular basis to ensure the systems are up to date and secure (*Network Based Vulnerability Assessment*).	1(h) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].	1(h) Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
It is recommended that:			
2(a) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Network & Service Discovery and Network Based Vulnerability Assessment)*; **Same as Recommendation No. 2(b) Phase III**	2a) A&E/ITSS concur with the recommendation and will work with Operations and Applications to ensure connectivity between network hardware does or continues to follow established security requirements for encryption of data, using tools approved for use by GoC lead agencies and industry standard practices where practical and applicable. Suitable technologies exist, and are implemented as requirements are identified.	2(a) Ongoing. New implementations as they occur, retrofits as they are identified.	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
2(b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Network & Service Discovery and Network Based Vulnerability Assessment)*; **Same as Recommendation No. 2(e) Phase II - below**	2(b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*].	2(b)Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 Nicole Gratton 956-8579 and Sr. DG, IT Operations - Dave Holdham 934-0341
2(c) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Network & Service Discovery and Network Based Vulnerability Assessment)*; **Same as Recommendation No. 1(d) Phase II**	2(c) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	2(c) March 2005	Sr. DG, TSD - Dave Adamson 956-5487 René Lalande 997-8693

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
2(d) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Network & Service Discovery and Network Based Vulnerability Assessment)*; **Same as Recommendation No. 2(e) Phase II - below**	2(d) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	2(d) Desktops by March 2005, other platforms to follow.	Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579
2(e) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Network & Service Discovery and Network Based Vulnerability Assessment)*; and **Same as Recommendation No. 2(d) Phase II - above**	2(e) ITSS are working with product and platform managers to implement hardening principles. As part of this effort, this recommendation will be addressed. Work is proceeding initially with standard departmental desktop computers, and will continue with other platforms. Responsibility will rest with the product/platform manager.	2(e) Desktops by March 2005, other platforms to follow.	Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579
2(f) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] (*Network & Service Discovery and Network Based Vulnerability Assessment)*.	2(f) ITSS are working with product and platform managers to implement hardening principles. As part of this effort, this recommendation will be addressed. Work is proceeding initially with standard departmental desktop computers, and will continue with other platforms. Responsibility will rest with the product/platform manager.	2(f) Desktops by March 2005, other platforms to follow.	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 Other A&E directors

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
It is recommended that:			
3(a) the 2001 firewall policy (including the appendices) should be reviewed, updated (if necessary) to reflect the current services offered on the firewalls, and brought out of draft mode *(Firewall Rules Assessment)*;	3(a) Systems concurs and will move forward and update the existing Firewall Policy to reflect the current and the N+1environments.	3(a) December 2004	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
3(b) HRDC should regularly review the traffic rules for support personnel and ensure that an appropriate change management procedure is in place in order to maintain a current and accurate list *(Firewall Rules Assessment);*	3(b) Systems continues to provide ongoing technical and engineering support to the teams responsible for Firewall support and rule implementation.	3(b) Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
3(c) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Firewall Rules Assessment)*; and	3(c) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	3(c) Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579
3(d) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Firewall Rules Assessment)*.	3(d) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	3(d) Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579 and Sr. DG, Operations - Dave Holdham 934-0341 Rocky Kreis 953-4470

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
It is recommended that:			
4(a) HRDC should review its current password policy, including its technical enforcement, and update them with the required changes to ensure strong password selection *(Password Assessment)*;	4(a) ITSS has presented a policy instrument, in draft, to ITSGC for review and approval regarding the use of Passwords that allow for access to the internal Departmental network. For technical considerations, refer to Phase I Recommendation No. 19.	4(a) March 2006	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
4(b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Password Assessment)*;	4(b) A&E concurs and supports a review of Passwords on other department systems to ensure compliance with departmental and industry standards/best practices. Processes, procedures and timelines will be provided by IT Security. These activities will be rolled into the periodic vulnerability assessments described in Phase I Recommendation No. 18.	4(b) A schedule will be published by January 2005.	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
4(c) regular password assessments should be performed to ensure compliance to the password policy *(Password Assessment);*	4(c) A&E concurs and supports a review of Passwords on other department systems to ensure compliance with departmental and industry standards/best practices. Processes, procedures and timelines will be provided by IT Security. These activities will be rolled into the periodic vulnerability assessments described in Phase I Recommendation No. 18. ITO concurs and the outcome will subsequently be implemented by ITO.	4(c) March 2006	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
4(d) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Password Assessment); and*	4(d) ITSS are working with product and platform managers to implement hardening principles. As part of this effort, this recommendation will be addressed. Work is proceeding initially with standard departmental desktop computers, and will continue with other platforms. Responsibility will rest with the product/platform manager.	4(d) Desktops by March 2005, other platforms to follow.	Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
4(e) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] *(Password Assessment).*	4(e) ITSS are working with product and platform managers to implement hardening principles. As part of this effort, this recommendation will be addressed. Work is proceeding initially with standard departmental desktop computers, and will continue with other platforms. Responsibility will rest with the product/platform manager.	4(e) Desktops by March 2005, other platforms to follow.	Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579
It is recommended that:			
5(a) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(a) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(a) December 2004	Sr. DG, TSD - Dave Adamson 956-5487 Brian Graham 994-3822
5(b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(b) Currently not planned	Sr. DG, TSD - Dave Adamson 956-5487 Brian Graham 994-3822
5(c) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(c) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(c) Implementation date to be determined on outcome	Sr. DG, Operations - Dave Holdham 934-0341 Rocky Kreis 953-4470
5(d) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(d) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	5(d) TBD	Sr. DG, TSD - Dave Adamson 956-5487 N. Gratton 956-8579

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
It is recommended that:			
* 1. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	A&E concurs, where practical and applicable, and will develop a "below the line" budget item.	March 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705
2. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	NVDS currently provides a [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] for employee remote access which meets the stated requirement.	Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579
3. HRDC's mobile device policy should be updated to address the issues of software installation by users, surfing the Internet for private use, updating software with current Security Patches and Service Packs, etc. *(Mobile Policy Device Review).*	Systems Branch agrees that these are important issues to be addressed. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. Further, while the new Wireless Policy Directive does not deal directly with the remaining issues, a number of other initiatives and policies do, including the Policy on the Use of the Electronic Network. However, recognizing the importance, Systems Branch will undertake to address these issues in the next iteration of the Mobile Device Policy Directive and/or associated Directives.	March 31, 2005	Sr. DG, TSD - Dave Adamson 956-5487 Bob Cloutier 953-3938 and Sr. DG, PSMP - Nada Semaan 997-1620 Carla MacIntyre 934-1733
Phase III			
a) **External Server Consolidation.** [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	March 31, 2005 Implementation date to be determined based on outcome	Sr. DG, TSD - Dave Adamson 956-5487 Brian Graham 994-3822 and Sr. DG, Operations - Dave Holdham 934-0341 G. Belleperche 997-4115

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
b) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	Sept 30, 2005 Implementation date to be determined based on outcome	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115
c) **Patching Vulnerable Systems.** Test and apply new patches as quickly as possible, first to critical systems, then to all other systems. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	A& E to fine-tune and review patch management protocols, lab reviews, processes, procedures and timelines. IT Ops already test and apply new patches as quickly as possible, first to critical systems, then to all other systems. Refer to Phase II (1a) and Phase I Recommendation No. 16.	March 31, 2005 Implementation date to be determined on outcome.	Sr. DG, TSD - Dave Adamson 956-5487 Brian Graham 994-3882 Sr. DG, Operations - Dave Holdham 934-0341 Rocky Kreis 953-4470

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
d) **Password Protection.** [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] Develop a user-awareness program that includes instructions aimed at reducing password reuse, particularly between systems of different realms and that use different authentication protocols (e.g. between Internet web e-mail services and sensitive Intranet applications). A sufficiently strong password policy should also be in place on all systems. The exact details of this password policy should be decided within the context of a threat-risk assessment.	Design, develop, operate Identity Management paradigm with timelines. ESS to implement outcome subsequent to IT Security timeline. Refer to Phase I Recommendation No. 19.	March 2006 Implementation date to be determined by outcome.	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115
e) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	June 30, 2005 Ongoing	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, Client Solutions - Ron Meighan 994-0749 Alain Lemay 994-0426

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
f) ***** [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act*.] [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	Design, implement, and operate zones-based enclave strategy in keeping with CSE Baseline Zones requirements document.	March 31, 2006	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115
g) **User-Awareness Security Program.** Develop a user-awareness program to address some of the issues outlined in this report, as well as provide points of contact for reporting problems that may be indicative of security breaches. Of particular importance is user-awareness programs on how to handle unsolicited e-mails, as well as e-mails containing suspicious attachments. [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	The Systems branch will develop and deliver increased education and awareness sessions, monitor for effectiveness and fine-tune as required. ITLS will work with ITSS once it is determined what the training requirements are.	June 30, 2005 The outcome will subsequently be implemented.	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, PSMP - Nada Semaan 997-1620 Rosa Gavillucci 994-1465

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
h) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] Further work in this area would be required. The outcome will subsequently be implemented by ITO.	March 31, 2005 If workaround cannot be established, target date identified above may not be achievable. Implementation date to be determined based on outcome.	Sr. DG, TSD - Dave Adamson 956-5487 Brian Graham 994-3822 Nicole Gratton 956-8579 and Sr. DG, Operations - Dave Holdham 934-0341 G. Belleperche 997-4115
i) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]. The outcome will subsequently be implement by ITO.	March 31, 2006 Implementation date to be determined based on outcome	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and Sr. DG, Operations - Dave Holdham 934-0431 Guy Belleperche 997-4115
j) [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	We are currently reviewing preventative measures/tools to help in mitigating further actions. The outcome will subsequently be implemented by ITO.	Dates to be determined once more is known.	Sr. DG, TSD - Dave Adamson 956-5487 Nicole Gratton 956-8579 and Sr. DG, Operations - Dave Holdham 934-0431 Murray Jaques 953-3398 or Guy Belleperche 997-4115

AED Recommendations	Corrective Management Action Plan	Expected Completion Date	Senior DG lead – Directorate Contact Name and Telephone
k) **Remove Unnecessary Banner Information.** [The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*]	[The information withheld qualifies for exemption pursuant to paragraph 16(2)(c) of the *Access to Information Act.*] The outcome will subsequently be implemented by ITO.	March 31, 2005	Sr. DG, TSD - Dave Adamson 956-5487 Dave Beach 956-9705 and René Lalande 997-8693 and Sr. DG, Operations - Dave Holdham 934-0341 Guy Belleperche 997-4115

Revision Document Name: My Documents: \IT Security Audit MAP AED Version Dec 21

Submissions from:
D. Beach, N. Deslauriers, N. Gratton, B. Graham, A. Lefebvre, C. MacIntyre, R. Kries, R. Poitras, R. Ramsay, D. Beckett, A. Lemay, R. Gavillucci, P.Charlsworth, J. Roberge, B. Cloutier, R. Lalande, G. Belleperche, R. Meighan, M. Snider, P. Lafrance, M. Jaques