Information Technology Security Audit and Review Overview

Prepared for: National Energy Board
444, Seventh Ave. SW
Calgary, Alberta, T2P 0X8

By: TRM Technologies Inc.
100, 151, Slater St.
Ottawa, Ontario, K1P 5H3

Date: 15th January, 2004

Contract No: 84084030164

DOCUMENT APPROVAL RECORD

Prepared by: _____

M. Harrop BSc. CEng. MBCS — Date
Senior IT Security Consultant

Reviewed by: _____

R. Moxley — Date
Director IT Security

Approved by: _____

E. F. Martin — Date
President, TRM Technologies

Table of Contents

Introduction

The revised Government Security Policy (GSP), which became effective in February 2002, requires that departments establish and implement a security program that covers administrative, operational, physical and personnel security as well as information technology security. While the policy will be supported by operational and technical security standards and minimum baseline security requirements (some of which are still in development), the new policy makes departments and agencies responsible for detailed implementation. In addition, departments and agencies must conduct their own threat and risk assessments to determine the need for safeguards above baseline levels specified in the policy.

As part of the new policy, departments and agencies are required to conduct active monitoring and assessments of their security program. In order both to assess policy compliance and to provide feedback as to the effectiveness of the new policy, departments are required to provide reports to the Treasury Board Secretariat on the results of these internal assessments or audits.

The National Energy Board (NEB) has undertaken a number of steps to enhance its IT security since the 1997 RCMP Security Evaluation & Inspection Team (SEIT) review. During the period 1st October and 15th December 2003, a Security Audit and Review was undertaken for the NEB project with the objective of providing an assessment of the overall compliance with GSP and NEB policy requirements as well determining the effectiveness of the implementations of the policies and supporting standards. The results of the assessment will provide the NEB with a comprehensive evaluation of how well it is succeeding in meeting the IT security policy and procedural objectives.

The assessment itself is documented in a full report that has been presented to the NEB. As the results of most security inspections contain potentially sensitive information that could be used by prospective attackers, it is usual to protect the findings of such inspections by marking the document in accordance with government classification requirements in order to ensure that circulation is limited to those with a “need to know”. In keeping with this common practice, the complete NEB inspection report has been accorded a PROTECTED designation. However, as it is NEB practice to place audit information on the public record wherever possible, this non-sensitive overview has been prepared in order to provide information about the nature and methodology used for the inspection and for the purpose of meeting a Treasury Board Secretariat requirement that it be informed of such inspections.

Executive Summary

This subject security audit and review that was undertaken for the National Energy Board (NEB) under the auspices of the Audit and Evaluation Committee in order to meet the monitoring and reporting requirements of the Treasury Board Secretariat (TBS). Under the Government Security Policy (GSP), departments and agencies are required to actively monitor and assess the effectiveness of their own security programs and to provide periodic reports to the TBS. This review was conducted for the NEB between October 1st and December 15th 2003.

Information technology (IT) is vital to the NEB's operations, and the effective protection of the IT assets (including data) is essential. However, new threats against information infrastructures are continually being identified and new types of attack are being initiated with increasing frequency. A comprehensive IT security evaluation of the NEB conducted by the RCMP Security Evaluation and Inspection Team (SEIT) in 1997 identified a number of deficiencies. Since that evaluation, steps have been taken to improve IT security. There have also been many changes in the Board's IT configuration as well as in the internal policies and procedures. The subject report provides the NEB with the results of a comprehensive, independent evaluation of how well the organization is succeeding in its meeting IT security policy and procedural obligations. The report will also help the NEB to identify areas where there are possible remaining weaknesses in approach and where there are opportunities to strengthen the security posture of the organization. (Please note that the focus of the review was limited to practices and procedures required by the GSP and related operational standards. This review did not include assessment of the specific technical security measures currently used by the NEB.)

The methodology used for this inspection combined a number of techniques. Checklists were developed to assess alignment with the Treasury Board Security Audit Management Guide and to evaluate compliance with the Government Security Policy, the operational standards associated with the GSP (i.e. the Physical Security standard, the IT Security Standard, and the Security Organization and Administration Standard), and related policies (the Policy on Electronic Authorization and Authentication, the Policy on the Use of Electronic Networks, and the Policy on the Management of Government Information). In quantitative terms, 234 criteria were examined to assess alignment with the Audit Management criteria, 57 policy requirements were examined to assess GSP compliance, and 167 factors were assessed in determining compliance with the related policies and operational standards. A physical site inspection was also undertaken and interviews were conducted with NEB staff members. The major findings are presented in narrative form in the body of the report and the detailed checklist and physical report findings are included as annexes to the report.

In addition to identifying areas where it may possible to strengthen the NEB's security posture, the report makes recommendations to improve security awareness and security management, and to encourage a culture of security awareness throughout the NEB.

The report emphasizes that maintaining effective security is an on-going task, not a one-time event.

In all, the report contains 34 recommendations that, if implemented, will help the NEB improve its overall security posture.

1. Overview of the NEB Security Audit and Review Process

1.1 Background

In February 2002, a new Government Security Policy (GSP) was introduced by the Treasury Board Secretariat (TBS). That policy requires departments and agencies to establish and implement a program covering all aspects of security including information technology (IT) security. Under the new policy, departments and agencies are individually responsible for determining how the policy will be implemented and each department is also required to actively monitor and assess the effectiveness of their own security program.

The last comprehensive review of IT security in the NEB was conducted by the RCMP Security Evaluation and Inspection Team (SEIT) in 1997. Since that review, a number of steps have been taken to improve security. There have also been many changes in the Board's IT configuration as well as in the internal policies and procedures since 1997. In addition, there has been a significant overall increase in awareness of the importance of safeguarding NEB IT systems and information.

In order to meet monitoring and review requirements, the NEB Audit and Evaluation Committee authorized this IT Security Audit and Review which was conducted during the period 1st October to 15th December 2003. The results of this independent examination of the NEB IT security environment provide an assessment of the overall effectiveness of current IT security procedures and of compliance with the requirements of the GSP and directly-related policies. In addition to providing the NEB with a comprehensive, independent evaluation of how well the Board is succeeding in meeting IT security policy and procedural obligations, the report will assist the NEB to identify areas where there are possible weaknesses in approach or implementation and where there are opportunities to strengthen the security posture of the organization.

1.2 The need to protect the NEB Information Infrastructure

Like most public and private organizations, in fulfilling its mandate, the National Energy Board is heavily reliant on information technology in general and on its information infrastructures in particular. Although IT security has always been a concern, recent advances in networking and online service delivery have greatly increased the risk of attack from outside the organization. In particular, widespread use of the public Internet has resulted in exposure to a wide variety of attacks (including worms and viruses, denial of service attacks, and attacks that compromise information holdings), as well as a very significant increase in the frequency of attempted attack. In addition to network-based attacks, new technologies (including wireless technology and portable storage devices) have resulted in opportunities for new kinds of attack and information compromise.

Given the high degree of dependence on IT resources and networks, effective security has become an imperative for the NEB. Security violations could cause degradation, disruption or even complete suspension of NEB business.

Although, in IT security, the greatest attention is typically paid to external threats, particularly those that can be realized remotely via the network, potential threats from inside the organization cannot be ignored. These can arise as a result of accidents, equipment failure, environmental failure, or from deliberate or accidental employee or contractor actions. While much effort must be put into protecting the perimeter of the IT domain from unauthorized intrusions, it is also important, therefore, to ensure that defensive measures and recovery mechanisms are employed to protect against the entire spectrum of threats, including threats from inside the organization.

1.3 The NEB Security Audit and Review

The subject NEB Security Audit and Review includes an assessment of compliance with GoC security policies and operational standards, plus a review of IT security in the NEB environment at the Tier 1[1] (security policy) and Tier 2 (operational standards) levels. The review excludes consideration of most Tier 3 (technical standards) aspects of security. (In this respect this inspection differs from the previous RCMP inspection which included Tier 3 considerations.) This review focuses on whether the requirements of the GSP are being met, whether the appropriate security policies and procedures are in place at the NEB, and whether the policies and procedures are adequate and are being followed. This review does not address detailed technical or configuration issues. For example, the review considers whether security mechanisms (such as firewalls & IDSs) are used but not whether the mechanisms are used or configured appropriately. Also, this review does not include any threat or risk assessment or any specific vulnerability assessment. As the task is directed towards IT security, other aspects of security covered by the GSP (such as

[1] Ref 1.11 defines security documentation in terms of three levels of standard: Tier 1 - Security Policy, Tier 2 – Operational Standards & Tier 3 – Technical Standards.

physical and personnel security) are not addressed except to the extent that they overlap with IT security concerns.

1.4 Methodology

Although various guides exist, there is no single agreed methodology for the various types of security inspection.[2] As a result security inspections tend to be quite individualistic even though they may have many commonalities. The particular methodology used for this security audit and review comprises several steps and draws on a number of guidance documents including the *Treasury Board Information Technology Security Audit Guide* (Ref. 1) and the documents listed under section 3 of the References.

The particular elements upon which this security inspection is based comprise existing NEB policies and documentation, interviews with NEB staff, inspection of the NEB site and processing environment, combined with a checklist approach to assess compliance with specific GoC requirements.

The Treasury Board Information Technology Security Audit Guide, (Ref. 1) which contains an audit checklist, was the starting point for the review. However, this document was last updated in 1996 and has not yet been revised to reflect changes to the GSP that came into effect in 2002. The checklist used in this review to assess security audit requirements is derived from the criteria in the 1996 Security Audit Guide but the checklist has been updated for this inspection to reflect both policy changes and the NEB requirement. In addition, supplementary checklists have been developed to assess compliance with the GSP, with relevant Tier 2 (operational standards and policies), and with a number of related policies, including the Policy on Electronic Networks and the Policy on the Management of Government Information.

The completed checklists, which are included as annexes to the report, stand as a permanent record both of the elements that were examined in the course of the inspection and of the resulting assessment. Completion of the checklists was achieved by a combination of inspection of NEB documentation, processes and environment, plus personal interviews with staff.

From inspection of the NEB documentation it was possible to obtain an indication of the extent to which GoC policy requirements had been formalized and the adequacy of the documentation. It was also possible to identify apparent gaps in the local policies and procedures.

Staff members with specific responsibility for security, development, record management and application development, as well as some end users, provided answers to questions arising from the inspection of the documentation and from the later physical inspection of the site.

[2] Federal government TRA's typically follow either the CSE methodology or the RCMP methodology though these are often adapted by the reviewing organization to meet local needs and organizational styles.

The interviews with selected staff members were a key part of the assessment as they provided an opportunity for those most directly affected by the policies and procedures both to provide input on the effectiveness of current security measures and to contribute suggestions regarding possible improvements.

Lastly, a physical inspection of the site was conducted.

The checklists were completed using information obtained from the above processes. In the interest of ensuring accuracy, clarification was sought from responsible managers and technical staff on individual points where necessary. Observations were compiled throughout the review process and incorporated into the narrative findings of this report. The findings take into consideration all the previously mentioned input. While the narrative largely follows the checklist topics, the findings also cover some topics that were not explicitly covered by the inspection checklists but which, nevertheless, were discovered during the inspection. Brief mention is also included in the report on some new areas of technology that are not yet reflected in the policies (e.g. wireless, active/mobile code and portable storage devices).

2. Findings

As noted earlier, the audit and inspection process involved a number of steps that included completion of a checklist developed from the *Security Audit Guide*, completion of checklists developed to assess compliance with the GSP and related Treasury Board Policies, and a physical inspection of NEB site facilities. The respective completed checklists and the Physical Inspection report are contained in Annexes A, B & C to this report and represent the "raw" findings according to the specific questions asked. Also, during the interviews and inspection process, additional relevant information was presented that did not fit into the questionnaires or the pre-determined list of physical security questions. Some of this information is reflected in the Physical Inspection report (Annex C) while the remainder, where relevant, is integrated into the analysis part of this section of the report along with an assessment of the implications of all the findings.

An evaluation of the findings of the inspection is divided into three sections. Firstly, there is a summary of overall compliance with government policy requirements, stated largely in quantitative terms, in order to provide a broad indication of how well the NEB is meeting the respective policy requirements. Secondly, there is a brief discussion on the findings exposed by using the Security Audit Guide checklist. Lastly, and most importantly, there is the analysis that takes into account the findings of all checklists, the physical inspection, and other information that came to light in the course of the review. The analysis section is largely structured according to the topics covered in audit checklist.

2.1 Policy Compliance

In the hierarchy of government security policies and standards, the Government Security Policy (GSP) is considered to be at the highest level (Tier 1); operational standards (such as the Physical, Personnel and IT Security Standards) are considered to be immediately below the GSP (Tier 2); and technical standards (such as the TSSIT) are at Tier 3. This hierarchy is illustrated in fig 1. This review assessed compliance with the GSP, relevant Tier 2 standards, and related IT security policies.

The policy compliance findings are summarized mainly in quantitative terms. While such a summary is helpful in providing an overall indication of compliance, and more particularly of indicating those parts of the policy where compliance is weakest, caution is needed in interpreting such quantitative data as it does not provide any indication of the relative importance of particular areas of non-compliance. For example, policy non-compliance in an area that is of low priority to the NEB at this time would likely rank very low on the risk scale, but non-compliance in some other areas may indicate a serious risk. The significance of non-compliance is discussed in the analysis part of the report.

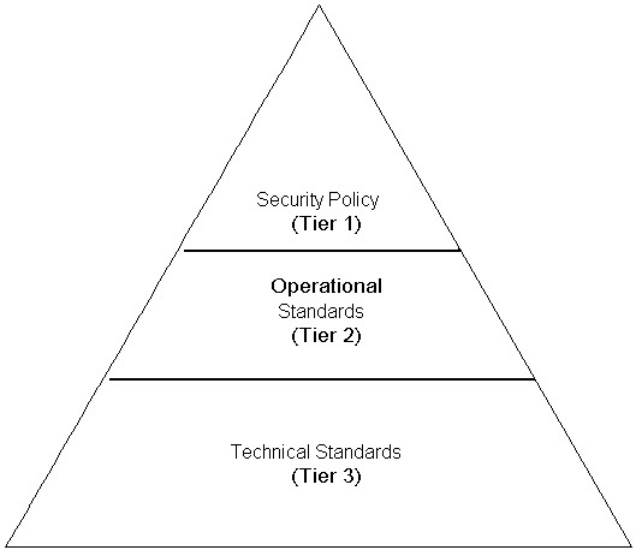

Fig 1: Hierarchy of government security documentation

2.2 Compliance with the Government Security Policy

In assessing overall compliance with the GSP, 57 requirements were specifically considered.

2.3 Compliance with the Operational Standards

Thirteen of the requirements of the Physical Security Standard were assessed along with 55 of the requirements of the IT Security Standard and 56 requirements of the Organization and Administration Standard.

2.4 Compliance with related policies

Rrelevant aspects of the Policy on Electronic Authorization and Authentication, the Policy on the Use of Electronic Networks and the Policy on the Management of Government Information were examined and the degree of compliance assessed.

2.5 Alignment with criteria of the Security Audit Management Guide

The Security Audit Guide checklist is not structured to assess compliance with particular policy or other requirements. It simply provides a way of assessing whether particular recognized good practices, as set out in the Audit Guide, are being followed and, if not, of identifying whether the practices that are being followed are equivalent, or are adequate as an alternative. The checklist also serves to highlight particular deficiencies. However, unlike policy compliance, there is no explicit government requirement to follow the Audit Checklist criteria, nor does failure to align with any particular part of the audit checklist criteria necessarily imply poor practice. In some cases the spirit of the criteria may be met in a way quite different from that envisaged by one or more particular criteria.

In quantitative terms, 234 criteria were considered in the Audit Checklist. Narrative included in the observations column of the checklist provides explanation of the reasons for any discrepancies.

To a large extent, the problem areas identified in the Audit Checklist correspond with issues identified in the policy and physical inspections. These are discussed in some detail, along with their implications, in the analysis part of the report.

2.6 Analysis of main findings of the inspection

The analysis section of the report provides a discussion of the main findings of the inspection. The section is, to a considerable extent, organized to align with the structure and headings of the Audit Checklist. However, the analysis covers the entire range of the findings of the inspection including items not necessarily covered in the checklists.

Analysis and findings are summarized in the report under the following topics:

- Organization and administration
- Status of ITS planning process
- Functional linkages
- Departmental ITS policies, practices and procedures

- Adequacy of ITS risk management methodology, procedures and capability
- Adequacy of information for risk decisions
- Use of departmentally-approved ITS risk management framework for IT development
- ITS risk management process for maintenance of operational IT
- Departmental procedures to control the authorization and access to IT systems
- Policies, practices and procedures for proper ITS equipment management, repair, maintenance and disposal
- Awareness of, and adherence to departmental repair and maintenance policies, practices and procedures
- Internal departmental ITS security audits
- Departmental IT security Threat and Risk Assessments (TRAs)
- Periodic CSE review of departmental communications security procedures and telecommunications systems
- Contracts with security requirements
- Initiation of ITS reviews, self assessments and internal security reviews
- Statements of Sensitivity and Modes of Operation documents for systems, networks and applications
- Personnel screening before being given access to systems/networks/applications that process sensitive information
- Revocation of access rights
- ITS training and awareness programs – all staff including users and managers
- Physical and environmental requirements
- Polices, practices, and procedures for IT hardware security & Configuration management of hardware
- Access control for remote hardware diagnosis
- Polices, practices and procedures for software security & for the use of privileged and powerful software
- Polices, practices and procedures for communications security & communications security requirements in IT development projects
- Network security polices, practices and procedures
- Use of appropriate safeguards in IT networks and network applications
- Policies and procedures for ITS Operations
- Shared information
- Staff responsibilities/issues of trust
- Electronic privacy concerns
- Classification of information
- Access to the Server Room
- Security event monitoring
- Teleworking
- Remote access
- Emerging threats and evolving technologies
- Interoperability standards and
- Management of information holdings

3. Conclusions and recommendations

Based on the findings of the report a total of 8 specific conclusions are presented along with 15 recommendations. A further 19 recommendations derive directly from the findings of the report.

Acronyms and Abbreviations

GoC	Government of Canada
GSP	Government Security Policy
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Technology Security
MGI	Management of Government Information
NCR	National Capital Region
NEB	National Energy Board
PC	Personal Computer
SEIT	Security Evaluation and Inspection Team (RCMP)
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
VPN	Virtual Private Network
WAN	Wide Area Network

References

The following is a list of documents referenced during the security assessment:

1. Government of Canada and Treasury Board Policies, Practices and Procedures

1.1 Audit Guide - Information Technology Security, TBS, 1996
1.2 Government Security Policy, TBS, February 2002
1.3 Policy on Electronic Authorization and Authentication, TBS, July 1996
1.4 Technical Security Standard for Information Technology (TSSIT), RCMP, Aug. 1997
1.5 Policy on the Management of Government Information, TBS, May 2003
1.6 Physical Security Standard, TBS Policy Manual Ch 2-2 (undated)
1.7 Personnel Security Standard, TBS Policy Manual Ch 2-4, Dec. 1993
1.8 Information Technology Security Standard, TBS Policy Manual, June 1995
1.9 Security and Contingency Management Standard, TBS Policy Manual Ch 2-6 (undated)
1.10 Policy on the Use of Electronic Networks, TBS, Feb. 1998
1.11 Security Organization and Administration Guide, TBS Policy Manual Ch 2-1, June 1995
1.12 Telework Policy, TBS, Dec 1999
1.13 Central Financial Management Reporting System User Guide, PWGSC, June 2001

2. NEB Policies, Practices and Procedures

2.1 NEB Security policy and procedures, July 2001
2.2 NEB Security Committee Organization Chart, June 2003
2.3 NEB Organization Chart, July 2003
2.4 SEIT Comprehensive Review of NEB, July 1997
2.5 Security: Acceptable Use of Computing Services Policy, July 1999
2.6 Acceptable Use of Computing Services, Questions and Answers (undated)
2.7 Asset Management Policy and Procedures, March 2002
2.8 Building Access Policies and Procedures, Nov. 2000
2.9 Contracting of Temporary Help Policy and Procedures, Feb. 2001
2.10 Contracting and Procurement Guide, May, 2002
2.11 Telecommunications Policy and Procedures, March 2001
2.12 NEB Information Systems Methodology V2.0, Sept 2002
2.13 Configuration Management, Release Management & Change Management Combined Function, Draft, 20th October, 2003
2.14 Recorded Information Security, Chs 10 & 11 of NEB Manual of Security Management, February, 1988.
2.15 Guidelines for the Handling of Sensitive Information, undated and unattributed.
2.16 Report on the Assessment of Threats and Risks, NEB, Dec. 1996
2.17 Central Financial Management Reporting System User Guide, Rel 3.2, Oct. 2002

3. Other documents referenced during the project

3.1 Management Planning Guide for Systems Security Auditing, National State Auditors and US General Accounting Office, Dec. 2001
3.2 Site Security Audit Checklist, G Halprin, SysAdmin Group, June 2003
3.3 Computer Security Audit Checklist, C.Rose, ITSecurity.com, April, 2002
3.4 Data Centre Physical Security Checklist, Sean Hearn, Sans Institute, Dec. 2001
3.5 Computer Security Audit Checklist, Chris Hardie, Summersault.com, April 2003
3.6 Guidelines on Active Content and Mobile Code, Wayne Janson, NIST Special Publication 800-28, Oct. 2001

Glossary of Terms

active code	code that can be transferred across a network and executed on a local system without explicit installation or execution by the recipient.
availability	the property of being accessible and usable upon demand by an authorized entity (IS 7498-2)
baseline controls:	a minimum set of safeguards established for a system or organization.
baseline security requirements:	mandatory provisions of the Government Security Policy and its associated operational standards and technical documentation.
confidentiality	the property that information is not made available or disclosed to unauthorized individuals, entities or processes. (IS 7498-2)
data integrity	the property that data has not been altered or destroyed in an unauthorized manner (IS 7498-2)
firewall:	an internetwork gateway that enforces a boundary between two networks and that is used to isolate, filter, and protect local system resources from external connectivity by controlling the amount and kinds of traffic that will pass between the two.
integrity	See *data integrity*
IT Security Zone:	an IT Security Zone is a networking environment with a well-defined boundary, a security authority and a standard level of susceptibility to network threats. Types of IT Security Zone are distinguished by security requirements for interfaces, traffic control, data protection, host configuration control and network configuration control.
malicious code:	programs that are written intentionally to carry out annoying or harmful action. They often masquerade as useful programs or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses, computer viruses, and worms.
mobile code	programs such as scripts, macros and other portable instructions that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
security audit	an independent review and examination of the system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security and to recommend any indicated changes in control, policy and procedures (IS 7498-2)
Secure Virtual Private Network (SVPN):	a VPN that uses cryptography (e.g. IPSec) (in contrast to a VPN based simply on logical isolation (e.g. MPLS or Ethernet VLAN).
Threat	a potential violation of security (IS 7498-2)
virtual private network (VPN)	a restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunnelling links of the virtual network across the real network.