Audit of the Time Information ManagEment (TIME) System

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

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

Date: **15th October, 2004**

Contract No: **84084040098**

A Word of Thanks

Completion of this task would not have been possible without the cooperation of staff members of the National Energy Board. TRM Technologies sincerely thanks all those who assisted us by providing the documentation and information needed to complete the task and by participating in the fact-finding interviews.

We would also like to thank the Project Authority, Mr Albert Fung, for his assistance in setting up interviews and obtaining the requested information.

DOCUMENT APPROVAL RECORD

Prepared by: M. Harrop CEng.
Senior IT Security Consultant

B. Falvo
IT Security Consultant

Reviewed by: ______________________________
R. Moxley PEng.
Director IT Security

Approved by: ______________________________
T. F. Martin PEng.
President, TRM Technologies

Acronyms and Abbreviations

BCP	Business Continuity Plan
CAB	Change Advisory Board
DNS	Desktop & Network Services (division of NEB)
DRP	Disaster Recovery Plan
EAA	Electronic Authentication and Authorization
ERC	Enhanced Reliability Clearance.
EXTRA	NEB Extranet (remote access system)
GoC	Government of Canada
GSP	Government Security Policy
HRIS	Human Resources Information System
IIS	Internet Information Services
IT	Information Technology
ITS	Information Technology Security
NEB	National Energy Board
PC	Personal Computer
PIA	Privacy Impact Assessment
SDM	System Development Methodology
SOS	Statement of Sensitivity
SQL	Structured Query Language
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
VPN	Virtual Private Network
WAN	Wide Area Network

TABLE OF CONTENTS

Executive Summary

This audit of the Time Information ManagEment (TIME) system was initiated by the National Energy Board (NEB) Audit and Evaluation Committee to ensure that adequate processing controls exist and that time-related information is accurate and timely for management purposes. The task was divided into two parts: a comprehensive review of the TIME system, its operating environment and security provisions in terms of the Government of Canada's Security Audit Guidelines, policy requirements and other best practice guides; and an independent review of the program code to identify any vulnerabilities based on the Microsoft Security Guidelines and recommended good security practices relating to .NET applications.

The audit has determined that there are no major weaknesses in processing controls for TIME though there are a number of areas that merit attention to reduce the possibility of potential future problems. The major findings are summarized below.

Systems Security: Network and system protection for TIME is generally effective as indicated in the Security Review and Audit conducted in 2003/2004 under the auspices of the Audit and Evaluation Committee (Ref 2.2). No evidence was found to suggest that new networking vulnerabilities have been introduced since the earlier review. The NEB network safeguards are fully adequate to protect the TIME system.

Continuity of Service: Although a Disaster Recovery Plan (DRP) has been developed for the NEB IT infrastructure it has not yet been implemented and there are no alternative processing provisions for TIME in the event of serious system failure. This requires attention, not just for the TIME system, but for the entire NEB information processing environment.

Risk Management: Overall risk management processes are appropriate but no Statement of Sensitivity (SOS) has been developed for the TIME data, which means there is inadequate information for making risk decisions. A Threat and Risk Assessment (TRA) has been conducted for TIME but we have been unable to confirm that the recommendations have been implemented.

Data Management: Data management and protection procedures are generally appropriate and effective, as are back-up procedures and data linkages to other systems. However, in the absence of a Statement of Sensitivity, it is possible that data is not being fully protected in accordance with Government of Canada requirements.

Incident Management: Procedures for problem and incident management are judged to be appropriate and effective.

Configuration Management: The current NEB configuration management provisions are fully adequate for TIME. The provisions made for the NEB network and IT fully meet the physical and environmental protection needs of the TIME system.

Change Management: Changes to TIME are appropriately controlled and managed. IT Security planning and participation in the TIME development process is judged to be adequate and effective. There is potential for future problems with respect to the way emergency changes to TIME are processed but recommendations are made to address this.

System Design and Coding: A number of vulnerabilities associated with the .NET program coding were identified but only two of these (the SQL-injection vulnerability and the exposure to Cross-Site scripting attacks) are considered high risk. Recommendations are included to address all the coding vulnerabilities identified.

Other Issues: While a number of other potential vulnerabilities are identified in the report, probability of these being exploited is judged to be low. It was also noted that, although timeliness of employee reporting has greatly improved, there is still some concern over late reporting and the ability to verify the accuracy of data that is very late.

TIME provides the NEB with an effective time management and reporting tool. Updating, reporting and review on a timely basis are now possible and identification of problems is easier than under the previous system. Accuracy of the data is improved by more timely reporting and, overall, the quality of the data should be much improved over that in the old system. The security of the data is at least as good as under the old system. In addition, TIME has enabled some new reporting policies to be implemented. While some tardiness in reporting remains, the system supports better overall control and should enable the NEB to base cost-recovery on more current information.

All potential vulnerabilities and areas of concern are highlighted in the *Findings* section of the report. Eleven recommendations are made which, if implemented, will address the potential vulnerabilities and improve the overall security of the system.

1. Background and Introduction

1.1 The TIME System

The National Energy Board's Time Information ManagEment System (TIME) is an on-line system that facilitates the reporting and management of employee time utilization by time type (regular time, leave, overtime, banked time etc), by project, by commodity, and against established NEB corporate goals. The system provides for weekly timesheet entry and approval and is used to facilitate cost recovery according to commodity type. The system also provides for capital cost tracking. TIME is used by management to track and approve employee time usage and to support specific business processes. The system can be used to develop reports related to time usage.

TIME was developed in-house to replace an interim Microsoft Excel spreadsheet system. Phase I of the TIME system became operational in June 2002 and provided basic time reporting functions to meet cost-recovery needs. A number of enhancements have been introduced since Phase I to increase the overall functionality and utility of the system.

TIME, which was developed in-house in 2002, is coded using Microsoft .NET technology and uses a Structured Query Language (SQL) Server 2000 database. It is linked to the Human Resources Information System (HRIS) via a Bridge application (also developed in-house) and is accessed by users over the NEB Intranet using web-browser technology. The system can also be accessed by employees from external locations via the corporate extranet (EXTRA).

1.2 Objectives and scope of this audit

The overall objectives of this audit were to ascertain that the system processing controls of the TIME system are reasonable and adequate to ensure the continued integrity and availability of data relating to the attendance and leave of NEB employees. This task included a comprehensive examination of the information system processing controls, in accordance with generally accepted good security practice and the Security Audit Guidelines of the Government of Canada, plus a detailed assessment of the system design and code in order to identify possible vulnerabilities and divergences from recommended good security practices relating to .NET applications.

Specifically excluded from this security audit are data networks, firewalls, routers and other network resources that are not specific to the TIME system. General system operations and off-site backup facilities were also judged to be out of scope as were ancillary systems (such as the Bridge application and Human Resources Information System (HRIS)) that interface to TIME or that provide data to TIME.

A comprehensive review and audit of NEB Information Technology (IT) security was undertaken in late 2003/early 2004 (Ref 2.2) and a Threat and Risk Assessment of the TIME system was conducted in 2003 (Ref 2.6). No attempt is made to duplicate or reevaluate any of the findings of these assessments but the results were taken into consideration to the extent that they impact the TIME system.

2. Methodology

2.1 Overall approach and methodology

The methodology used for this review relied on a combination of techniques that included site visits and off-site reviews, examination of available documentation (including the actual code), review of previous inspection and assessment results, interviews with key staff, and evaluation against recognized good IT security and security audit practices.

The work was divided into three main phases as follows:

Phase 1: Planning and initial review

- Gaining an initial understanding of the information management environment and the TIME system.
- Reviewing Government of Canada security audit and inspection requirements for IT systems and identifying the sections of the requirements that were relevant to this review;
- Preparing an audit checklist based on the above;
- Developing an approach to the assessment of the TIME program (design and code);
- Conducting an initial review of preliminary documentation supplied to us before the site visit and identifying gaps in the documentation;

Phase 2: Site visit and in-depth system review

- Conducting interviews with key staff;
- Identifying any gaps in the documentation or additional relevant documentation;
- Conducting a thorough review of available documentation on the TIME system including background information and relevant statutes, policies and procedures and documentation regarding the TIME system;
- Obtaining clarification on issues arising from the interviews and documentation;
- Viewing a live demonstration of the system and its capabilities;
- Conducting a detailed examination of the system code and controls;
- Developing a detailed approach for the analysis and reporting phase.

Phase 3: Analysis, evaluation and reporting

- Assessing the information gathered in Phases 1 & 2 and, where necessary, seeking additional information;

- Analyzing and evaluating the information gathered in terms of required IT security audit and controls;
- Identifying any deficiencies;
- Documenting the findings in an audit report with specific recommendations to address the processing control gaps identified;
- Presenting the results in a draft report to the NEB Project Authority; and
- Reviewing (and revising as necessary) the draft report following NEB review and developing the final report.

As indicated in the Statement of Work and the Action Plan, the specific elements of the TIME system considered in this review included: Continuous Service; Systems Security; Configuration Management; Problems and Incidents Management; Data Management; and Change Management. In addition, Risk Management and Other Issues were considered.

2.2 Assessment of the TIME application

Assessment of the TIME program itself included a demonstration of the application, a walk-though of the system and development infrastructure with one of the developers, and a detailed review of the design and code. Pages, custom components and application objects were identified to help gain an understanding of the development approach.

The code was then reviewed to evaluate all areas of the application where security could be a concern, in particular, development techniques, security countermeasures and deployment and configuration.

2.3 TIME operating environment

The review of the TIME operating environment and practices consisted of an assessment and evaluation of all aspects relevant to the TIME system itself, its data and its interactions, within the context of the overall NEB operating environment.

All available documentation was reviewed, including design documentation, report formats, business rules, operating procedures, error messages, user satisfaction surveys, conversion procedures, test documents and test results. Interviews were conducted with key staff and follow-up questions were submitted by e-mail and telephone.

Criteria for assessment were based on relevant sections of the Treasury Board Security Audit Guide, criteria derived from other security audit and best practices guides (particularly Refs 3.3, 3.4, 3.5 and 3.6) and security policy and best practices requirements applicable to individual systems.

The extent to which the TIME system meets (or does not meet) the criteria was assessed on the basis of the interviews, the documentation provided and an assessment of the programming and design characteristics of the system.

3. Findings

3.1 Functionality of the TIME system

The time management process that preceded the TIME system, the Time Reporting Interim Procedures (TRIP), was developed as a short-term measure to address Y2K concerns. It relied on manual inputs to an Excel spreadsheet. The process involved many steps and there were many opportunities for delayed input. In addition to the timeliness problem, the spreadsheet data was becoming corrupted and it was becoming impossible to record time accurately. It was a costly, inefficient process and deployment of TIME was expedited to try to overcome these problems.

With the on-line TIME system, each employee is required to report their time for the previous week by each Tuesday morning. If an on-line timesheet has not been submitted, an e-mail reminder is sent out after one day. The respective Team Leader is notified of time sheets that are still outstanding after one week. All outstanding timesheets are also included on the Team Leader's "To do" list. (Currently, there is no escalation above the Team Leader.) Timeliness of timesheet submission is generally much better under the TIME system.

The TIME System Administrator produces quarterly reports that show the number of outstanding timesheets by business unit.

Individual opportunities for mis-reporting are limited (and are no worse than with paper reporting). For example, an individual may mis-report time worked, overtime, leave taken or banked time. Ultimately it is up the Team Leaders to check that staff are reporting accurately. Because timesheet submissions are generally more timely, there is much greater probability that any misreporting will be detected.

Access to the TIME data is granted according to position. Employees have access only to their own data. Team Leaders have access to their employees' data for verification, approval and planning purposes.

Team Leaders are responsible for review and approval of input data and leave and overtime reporting. HR staff and Team Leaders use the data for the preparation of HR reports. HR staff also use the data to support investigations.

The TIME system has clearly helped to overcome many of the problems of data quality and timeliness of reporting that were experienced with the old system. Employee surveys taken after the introduction of the TIME system indicate a high level of user acceptance and satisfaction with the system.

3.2 Overall adequacy of the processing controls of the TIME system

3.2.1 Continuity of Service

There is currently no Business Continuity Plan (BCP), contingency plan, or disaster recovery procedures for the TIME system itself. A Disaster Recovery Plan (DRP) has been developed for the NEB IT infrastructure as a whole but has not yet been implemented. *There are no alternative processing provisions in the event of serious system failure.* This requires attention, not just for the TIME system, but for the entire NEB information processing environment.

TIME data is backed-up daily from the server to tape. Tapes are sent off-site monthly and held by Library and Archives Canada for 26 months. The current routine backup and recovery procedures for the SQL server, and the frequency of backups, fully meet the needs of the TIME system.

The impact of a severe system failure on the TIME system would depend on the duration and severity of the failure. A failure of less than seven days would likely have minimum impact (e.g. there would likely be some delay in reporting) but the impact would likely grow with the duration of the failure. There is no provision for reverting to paper processes so time reporting would simply be held up until the system could be restored.

While other systems would likely be impacted to a greater extent than TIME by severe system failure, the lack of an operational BCP and DRP represents a serious weakness and fails to meet government objectives with respect to continuity of service provisions.

3.2.2 Systems Security

To a very large extent, the security needs of the TIME system are addressed by processes and procedures put in place by Desktop and Network Services (DNS) to address the security of the NEB network, the workstations and the remote access service.

<u>Procedures to control the authentication, authorization and access to the TIME system</u>

The design approach to TIME focussed on authentication and authorization of the individual in order to ensure appropriate access rights to the TIME database. Authentication and access rules are governed by NEB network authentication and access requirements in addition to the specific requirements for the Time system authorization and access. Access to TIME is via the normal NEB Intranet log-on or via the EXTRA log-on provisions. Electronic authentication is provided via password-protected access to the corporate Intranet and by tokens and passwords for remote (EXTRA) access. Access to TIME is restricted to NEB employees who are required to have Enhanced Reliability Clearance (ERC). Network access is granted to employees by DNS staff at the request of the employee's supervisor and access is revoked as part of the exit procedures. Access control is based on roles and separation of duties: access rights are determined according to the position/role of the user. Access rules, which are defined in the Business Rules document (Ref 2.11), provide for the management of project codes.

If an employee is absent, the TIME System Administrator can delegate their access rights following consultation with the respective Team Leader. Some of the executives have also delegated access to their administrative assistants. Where someone is acting in a position (whether paid or not), access may be delegated and this is recorded in the HRIS. Acting access continues for one week after the return of the incumbent to allow for verification of timesheets covering the final week of incumbent absence.

Apart from access for reporting (which is available to all employees) and management, special access rights exist for some Finance staff (for reporting and cost recovery purposes), designated Systems staff (for entering capital access codes), the HR Advisor (for staff relations and investigations e.g. reviewing patterns of sick leave). Also, the System Administrator and 3 members of the HR staff have access to administer the system and to retrieve reporting data and input it (manually) into the HRIS. (The System Administrator cannot change the data on a time sheet but can wipe it out completely.) In addition, the Chief Operating Officer's administrative assistant has access to review non-compensatory time reports.

External access to TIME is via the EXTRA system and uses RSA tokens and SSL via a CITRIX server. Access is through a password and PIN. There are currently 150 hardware tokens and 140 active accounts. A TRA was conducted on the EXTRA system in September 2003 and there are reported to be no unresolved issues or vulnerabilities in the EXTRA system that could impact the TIME system. (We did not review the results of the EXTRA TRA in this review as it was beyond the terms of reference of the project.) A standard was developed for EXTRA to address identification and authentication mechanisms and a policy was created to address usage.

Revocation processes are generally effective. Network access is revoked as part of departure procedures. Access may also be revoked for other reasons on an individual basis. Access to the network by contract employees is limited to the period of the contract (though only NEB employees have access to the TIME system itself).

Procedures and controls governing authentication, authorization, access and revocation are judged to be completely satisfactory for the TIME system.

Currency and communication of policies and procedures

Procedures governing the use of TIME are captured in the Intranet-published TIME 3.0 Help document (Ref 2.3) which also provides a record of up-dates to the system. The Help document is a comprehensive and effective mechanism for guiding users and informing staff of routine changes. It is the primary communications mechanism between TIME development staff and users, though e-mails are also used from time-to-time.

Overall, procedures documentation is judged effective and adequate for the system.

Polices and procedures for software security

Software security provisions applicable to the TIME system are addressed to some extent in the System Development Methodology (SDM) and more generally in the overall NEB Security Policy Framework and the applicable TBS and NEB HR policies. Collectively these provide sufficient guidance to designers, programmers and users to maintain the appropriate level of software security.

Polices and procedures for communications security

All TIME use is via the corporate Intranet or through the EXTRA system.

The NEB's network security practices fully meet the needs of the TIME system and there is a good level of compliance with these procedures.

Use of appropriate network safeguards

Appropriate network safeguards are in place and staff members are very aware of the need for effective network protection. All networking is internal except for the remote access provisions described earlier.

A GTIS-managed firewall is used to isolate the internal network and data from the public Internet. All network and workstation traffic is subject to scanning for viruses and malicious code and EXTRA users are required by policy to install approved anti-virus and firewall software on any system that is used for EXTRA remote access.

The NEB network safeguards are fully adequate to protect the TIME system.

3.2.3 Risk Management

Adequacy of information for risk decisions

No Statement of Sensitivity (SOS) has been developed for the TIME data, nor has a Privacy Impact Assessment (PIA) been conducted. It has been suggested that this is because the data did not change with the move from a paper process to an electronic process. However, there was no SOS (or PIA) when the paper process was in effect.

Because of the lack of an SOS and PIA, there is inadequate information for making risk decisions.

NEB staff are assuming that the TIME data is designated (Protected B or lower) but it is known that some of the personal data is extremely sensitive. Although processing provisions meet the required level of protection for Protected B data, without an SOS, there will always be a degree of uncertainty about the sensitivity of the data. An SOS would provide the basis for ensuing that the data is appropriately protected and handled.

Adequacy of departmental ITS risk management framework and methodology

The NEB uses a Facilitated Risk Assessment Process (FRAP) which provides for peer review during system development. Except for the lack of an SOS, adequate provision was made for security during the development phase of TIME and the IT Security Coordinator was consulted during the early stages of the project.

There are no special security maintenance requirements for TIME beyond those specified within the overall NEB Secuity Policy and Framework and the System Development Methodology (SDM).

When TIME was first developed in 2002, the SDM did not include specific requirements for security or privacy. Security was addressed by consulting with the IT Security Coordinator and was designed to match business requirements. The SDM has since matured considerably. System development and review processes now require that the security requirements be considered during the design and development stages.

Overall, the security risk management process is judged to be adequate and effective for the TIME system. The development process, while not completely fulfilling the objective of following a single recognized SDM, is judged to have been appropriate given the status of the NEB SDM at the time of the initial development.

Threat and Risk Assessments (TRAs)

A TRA of the Time system was conducted in 2003 (Ref 2.6) and the results reviewed in an internal presentation in January 2004 (Ref 2.7). *We have been told that there are no unresolved issues or vulnerabilities resulting from that TRA but we have not been able to confirm, either from interviews or documentation, that all risks identified have actually been addressed at this point.* Furthermore, there has been a change in the TIME staff responsible for addressing these recommendations. It is suggested that there be a further review of the TRA findings to confirm that all identified vulnerabilities have been adequately addressed.

Of the related systems, as noted above, a TRA was conducted on the EXTRA system in 2003. *No TRA has been conducted on the HRIS or the Bridge system.*

3.2.4 Data Management

The TIME data is held in an on-site SQL cluster managed by CGI Inc. Source data validation is done at several levels. Timesheets cannot be submitted if they break any of the Business Rules (Ref 2.11). There is checking to protect against invalid combinations of data (e.g. banked hours cannot be entered during periods of sick leave). Errors associated with accuracy of data (e.g. hours submitted) can be detected only by the Team Leaders who check for reasonableness and for any obvious errors.

During the initial system roll-out and the changeover from the Excel spreadsheet system, data administrators validated all data and contacted employees if anomalous data was found. All employees were asked to check their own timesheet data (as specified in the Test documents).

TIME data is retained indefinitely within the system and is backed-up off-site.

Data linkages

TIME data is entirely internal. No data is automatically exchanged with other systems.

The primary linkage is to the Human Resources Information System (HRIS) which has data common to all HR applications (e.g. name, position, supervisor and periods of absence.) The tombstone data used by TIME is in the HRIS but there is no direct link between TIME and the HRIS. Information flow between TIME and HRIS is uni-directional (i.e. data flows are exclusively from HRIS to TIME – no data flows directly from TIME to HRIS). Information is transferred via the Bridge application, a system that was developed in-house and that serves other systems in addition to TIME. If the HRIS or the Bridge system failed there would be no live connection through which new employee data could be obtained.

Because of the limited data flows and the fact that functional linkages are exclusively "in-house", the risk to TIME from these linkages is judged to be low. *However, neither the Bridge nor HRIS has undergone a TRA.*

Data protection

Transaction authorization and access to data are governed by the provisions of the system as defined under Roles, Responsibilities and Permissions as documented in Ref 2.3. From an operational standpoint, only a limited number of staff have system access that allows permissions to be changed. (Specifically the System Administrator, though potentially the software maintenance programmer as well). In general, employees are prevented from accessing screens unless they are authorized to have access. The system has some built-in checking to ensure that entries are "credible" (e.g. not allowing certain combinations of reporting) and the system will not allow inputs if the system detects specific warnings, but it is up to Team Leaders to monitor the accuracy of reported time.

User account management and review are under the control of the System Administrator, though the Team Leader, Information Systems has access to the TIME for the purpose of entering capital access codes. System access privileges to TIME are created by the IT group at the request of the TIME System Administrator. These processes are potentially vulnerable, particularly if someone gained access to the System Administrator's account, but the fact that access to the system is limited to NEB employees and access is exclusively via the corporate Intranet or EXTRA system reduces risk to a manageable level. However, it is extremely important that those with privileged access carefully guard their passwords and ensure that non-trivial passwords are used. Token access (rather than password access) for privileged users would further reduce the risk associated with password compromise.

TIME data is assumed to be Protected B or lower but no SOS or PIA has been done to confirm the sensitivity of the data. *Contrary to policy, data is not marked, even when it appears in a printed report.* This is likely because of uncertainty over the sensitivity classification. Within the server environment, processing is conducted in facilities that equate to a minimum of Protected B level. System backups are marked Protected B using specially-developed labels.

3.2.5 Configuration Management

TIME runs on the NEB standard workstation/network configuration. If any configuration changes are required, they are reviewed and approved by the Change Advisory Board [1](CAB) and documented on the Information Management Business Unit area of the F drive.

During the initial TIME deployment, problems were encountered with some particular desktop configurations. These were all resolved following the initial 2-month period. The software now runs on all systems.

The current NEB configuration management provisions are fully adequate for TIME.

<u>Physical and environmental security requirements</u>

TIME does not have physical or environmental requirements beyond those relating to the overall NEB environment, the corporate network and the extranet access. Physical and environmental requirements were considered in the design and development of the corporate network and the EXTRA system. In addition, the participation of the IT Security Coordinator in the design review process for TIME ensured that any specific needs in this area would be addressed.

The provisions made for the NEB network and IT fully meet the physical and environmental protection needs of the TIME system.

3.2.6 Change Management

<u>ITS planning</u>

As reported in Ref. 2.2, the NEB has an effective security management infrastructure in place.

[1] CAB members include the CIO, IT Security Coordinator and Information Systems and DNS Team Leaders.

IT Security planning and participation in the TIME development process is judged to be adequate and effective.

<u>System maintenance</u>

There are no plans for further development of the TIME system, other than adaptive changes.

Procedures in effect for systems software maintenance, change initiation and control are set down in the Change Advisory Board (CAB) procedures (Ref 2.12). System maintenance procedures are loosely defined in the SDM and maintenance roles are defined. For scheduled system revisions or upgrades, an impact assessment is prepared by the person proposing the change. The proposal is then presented to the CAB which reviews the proposed change and validates the proposal. All CAB change proposals are retained on the F drive.

The procedures for documentation of changes call for comments to be inserted along with the code. Enhancements are summarized along with version/release number in the Help file.

A pre-production system is used to test proposed changes to the production system. Once a change is approved and tested, transfer to the production environment is approved by the CAB. There are generally no code reviews prior to production except by the original programmer, but the TIME system code has been reviewed during this audit.

There is no specific software release policy. Changes to the TIME system are made as needed, though in general non-urgent changes are grouped and released quarterly. Emergency changes are implemented immediately following informal consultation with affected staff.

While this process appears to be working well we noted two potential problem areas. First of all, CAB authorization is required only for major changes. Minor updates and emergency changes are not reported to the CAB and rely on informal monitoring only. Urgent changes are coded and tested by the programmer and then tested by the TIME System Administrator. Such changes do not go to the CAB and the only documentation consists of explanatory e-mails between the developer/programmer, production staff and the TIME System Administrator. Secondly, the TIME system code contains comments for only some of the code. These issues are not currently causing any problems but could give rise to problems if there are staff changes or if, in the future, there is a need to investigate the history of past revisions.

There is also concern with the updating process, particularly with respect to non-scheduled changes. The production environment is locked down and developers do not have access to the production environment. When access to the production environment is required (e.g. to run a development script), the developer asks a specific member of the production staff to run the script. Scripts are usually delivered on a floppy disk and the *production staff member is given a brief explanation of what the code is to do. However, no record is kept of either the request or the script. Up to now only two members of staff have been involved in the process. However, this process does not appear to be documented in any formal procedures. The process is very informal and relies on trust between the respective staff members. The lack of any documentation of the request or the script could cause significant problems at a later time, particularly if there are staff changes.*

3.2.7 Management of problems and incidents

If the system goes down, or if problems are detected, the Service Desk is the first point of contact. The Service Desk maintains an incident log on the HEAT system. Network incidents are handled by DNS staff. Issues with the TIME system are passed to the responsible development group. The specific response depends on the nature of the incident. The IT Security Coordinator is made aware of security-relevant incidents.

There is no explicit TIME system audit trail as such but there is tracking data that can serve to provide a history of who did what to each time sheet and when. Time-stamps are made of each system update and there is a record of changes made to the system. (As noted above, this record does not include information about emergency changes.)

Incident handling is addressed at a number of levels. Automated identification of operational events is provided by Big Brother which flags the potential impact of events as high, medium or low impact. There is also a systematic manual review of server event logs for anomalous behaviour. A Tripwire intrusion detection system is in the process of being implemented. From the standpoint of administrative controls, all employees are required to use only their own accounts and to lock their workstations when unattended.

Attacks against the TIME system by authorized users (employees) are not considered to be a major threat. The most likely type of such incident (misreporting on the part of employees) would have a high probability of detection through the review and reporting procedures that are built into the system. To date, examples of employee misuse of the system have been rare. If detected, incidents are addressed by standard disciplinary procedures.

Procedures for problem and incident management are judged to be effective.

3.2.8 Other issues

No incidents involving TIME system security have been reported so far. The major concerns identified by NEB staff during the interviews were over possible risks to the integrity and consistency of TIME data. *The biggest risk to the integrity of the data is that of malicious tampering, though the probability of this threat being realized is judged to be remote.* Those who are authorized to have access to the TIME system have little motivation to manipulate the data maliciously.

Attacks from external sources would require hacking into the system through the firewall or the use of a compromised system to gain access. Safeguards against such attacks are in place via the standard NEB network protection measures but motivation for external attacks against TIME data is believed to be low.

There is potential for backdoor access to the system by knowledgeable personnel. Such access could result in changes to access rights (e.g. if the Bridge were compromised, it would be possible for a knowledgeable user to change the reporting structure.) Once again though, motivation for such attacks is believed to be low.

The TIME system is the first .NET/SQL application developed for the NEB. This legacy is, to some extent, reflected in the system design and some of the legacy-system practices are retained in the current system.

There is a potential problem over the possible mis-configuration of access rights through manual processes but this is more likely to happen as a result of errors during the input process than through a deliberate attack.

Although the system has greatly improved the timeliness of employee reporting, there is still some concern over late reporting. It is difficult for the Team Leaders to verify the accuracy of data that is very late. It is also reported to be difficult to convince staff of the importance of submitting data on time. Some of this tardiness may be attributed to a lack of understanding by staff of the primary function of the TIME system (i.e. cost recovery facilitation).

3.3 Review of the TIME system design and coding

This portion of the audit focused on the system design and program code of TIME, which was developed in Visual Studio.NET. The application is assessed against the recommendations of the Microsoft .NET Security guideline. Potential security risks were reviewed within the application code, its hosting environment, and the data environment. All areas of vulnerabilities most commonly found in web applications developed in ASP.NET were reviewed. Lastly, SQL Server and IIS configurations were examined to confirm that security requirements for these components have been addressed.

The approach used in this part of the report is to provide a brief description of the features used to support the security needed for each aspect of the system being reviewed. This is followed by the particular observations on the features as they relate to the TIME system. Where potential security vulnerabilities are identified, recommendations are made to mitigate the risk.

3.3.1 Cryptographic techniques

Cryptographic techniques are used to transform data to protect its confidentiality and/or its integrity. Techniques include encryption, i.e. the process of hiding information to protect its content by using a reversible cryptographic algorithm, and hash functions that are used to produce an irreversible cryptographic digest of information to confirm its integrity. Microsoft Windows and the .NET Framework include robust encryption algorithms.

The TIME system does not need to make much use of cryptography. Due to the nature of the application, there is no need to encrypt data passed from the client. TIME makes appropriate use of secret key encryption to prevent the exposure of the trusted user accounts and passwords to the databases.

3.3.2 ASP.NET Authentication & Authorization

Authentication confirms the identity of the individual, while authorization controls the specific operations that a user may perform.

TIME makes appropriate use of Windows Integrated Security to authenticate users and to provide access to the application. All users who have a Windows account for the domain have access TIME. If a user attempts to launch TIME without having logged onto the network, they are prompted to enter a username and password for a specific domain.

The TIME authentication process requires both Windows authentication, and confirmation that the user exists in the Common database.

TIME does not use the built-in ASP.NET capabilities to authorize authenticated users. Instead, it uses a form of custom-built authorization routines. This constitutes a secure and recommended approach that provides similar functionality to the ASP.NET capabilities.

Although TIME makes use of the built-in Windows authentication capabilities, it does not take advantage of the built-in role-based authorization features. Instead, TIME manages its own roles with custom-built components. The built-in ASP.NET support for role-based authorization would have simplified authorization in some cases and could have minimized coding efforts. That being said, the technique used does not create any security vulnerabilities.

3.3.3 Application Attacks

Generally, attacks on shared networks or Internet systems and applications are launched at two different levels: system and application. This review focused on application-level attacks and areas where .NET applications are vulnerable to attack.

SQL-Injection attacks

An application is vulnerable to attack if unchecked user input is used as part of the SQL string that is constructed to form the final SQL statement. Embedded SQL is used throughout the entire TIME application code.

Cross-Site Scripting

TIME does not make use of any of the HTML and URL encoding techniques but makes extensive use of embedded SQL calls with constructed SQL strings built with variables containing unchecked user input. This, combined with the fact that TIME was developed and compiled in .NET 2002, results in TIME being vulnerable to cross-site scripting attacks. By default, systems compiled with .NET 2003 are protected against cross-site scripting attacks.

The TIME application is highly susceptible to both SQL-Injection and Cross-Site Scripting attacks.

Various techniques can be applied to prevent TIME from being vulnerable to both SQL-injection and cross-site scripting attacks.

<u>Defensive techniques for SQL-Injection Attacks</u>

A number of procedures can be followed to protect against an SQL-injection attack. At a minimum, TIME should validate input parameters and use parameterized queries. In addition, the use of stored procedures should be considered as the recommended approach. However, embedded SQL has been used throughout the application, therefore, validating input parameters and using parameterized queries would be just as effective and less time consuming.

<u>Defensive techniques for Cross-Site Scripting Attacks</u>

Some simple techniques can be used to prevent cross-site scripting attacks. Input that is being displayed as part of an HTML page can be protected using *Server.HTMLEncode*. Input that is being used as part of a URL, such as a query string value passed to another Web page, can be protected using *Server.UrlEncode*. Additionally, the content and length of input can be validated by using the ASP.NET validation controls.

Web applications coded in .NET 2003 are automatically protected from cross-site scripting attacks. Converting and deploying the TIME application as a .NET 2003 product would significantly decrease the current cross-scripting attack vulnerabilities.

3.3.4 Validation of Input

ASP.NET provides controls for validating both the client and the server but the TIME application makes very little use of the ASP.NET control validators. TIME provides a form of server-side validation but client-side validation should serve as a first line of defence. The ASP.NET validator controls are provided to facilitate client-side validation before user input gets passed to the server. This type of validation helps in preventing needless round trips to the server in order to provide validation error messages caused by malformed input values.

TIME provides server-side validation for the event generating the request. The input values are then validated within the code logic and handled appropriately. This method of validation does not give rise to any security risks.

Although the validation methods currently used in TIME do not pose a security vulnerability, ASP.NET validator controls should be used where appropriate. These controls are simple to implement and serve as an added measure of defence even if the code logic itself handles validation. At the very least, validation controls could help minimize the amount of code required by the server-side validating routines.

3.3.5 Exception Handling

Although software is created to run in an environment where everything is set up to work perfectly, ultimately software will be faced with a less-than-perfect environment where anything can go wrong. From a security perspective, software flaws are not only an annoyance but may also be vulnerabilities that can be exploited by an intruder to attack the software or the system it is running on.

Designing software to handle exceptions gracefully serves two purposes: it protects against attacks and makes for a more robust and satisfying user experience. Exceptions can occur anywhere in code, but most commonly they show up when a situation occurs that the developer did not originally anticipate and that the program logic does not handle with grace.

Error handling within TIME does not represent a security vulnerability. Local routines are implemented in most procedures to handle unanticipated exceptions. TIME has a global exception handling routine that handles exceptions that occur due to unforeseen circumstances. TIME makes uses of the .NET feature to automatically direct the user to a generic error page when un-trapped exceptions occur. This error page also displays the type of exception and detailed error information to users with privileged access.

Overall, the TIME application does a good job in handling local and global exceptions and this aspect of the application code does not need to be revisited.

3.3.6 Locking Down Windows, IIS, and .NET

Locking down Windows, Internet Information Services (IIS) and .NET means restricting services used by the application and making configuration changes to turn off unused services. The platform has to be locked down is because, while the platform itself may be secure, the default installation may not necessarily be secure.

Microsoft provides three automated tools for locking down Windows and IIS but these are not currently being used.

No automated lock-down tools were used in the TIME system to lock down Windows or IIS. These tools, while not absolutely required, do help to identify any potential security risks.

Although TIME is not directly exposed to the public Internet, it is recommended that automated tools be used to help lock down Windows and IIS to remove a number of residual risks. The effort to do this is minimal.

Microsoft also recommends that domain controllers always be isolated. For the Time system this is not a severe threat as most residual security vulnerabilities pertain to individuals within the organization. However, it is considered good practice to avoid having the domain controller also providing other types of network services such as print services, databases and IIS.

3.3.7 Securing the Database

The basic database security concepts are exactly the same as the concepts for securing an application, i.e. authenticate, authorize, and lock down. A number of steps can be taken to improve security of the SQL Server. These are set out below.

SQL services should be run under a low-privilege domain user account to ensure that, even if an intruder does manage to break in and take over the SQL Server machine, he/she will be restricted to a domain account that has few privileges.

If an intruder gains access to SQL Server and has permission to execute xp_cmdshell, he/she can do anything the SQL Server service account is permitted to do. For this reason, it is recommended that *xp_cmdshell* be removed unless it is absolutely necessary.

The Audit function will show whether people are trying to break into the database but it is not currently enabled. It is recommended that the Audit level option *All* be selected.

3.3.8 Overall conclusion from the review of the TIME system design and coding

Of all the risks that have been identified in this part of the review, only two are actually considered high risk. The remainder can be considered a low risk. Given the fact that TIME is an Intranet application and is already well protected from the outside world by a firewall and other network security measures, the threat level for most of the vulnerabilities mentioned in this report is quite low.

The two security vulnerabilities that definitely merit attention are the SQL-Injection vulnerability and the exposure to Cross-Site scripting attacks. The cross-site scripting vulnerability can be easily addressed by upgrading TIME to .NET 2003. Addressing the SQL-Injection vulnerability would require a little more effort but can also be done quite easily.

4. Overall Conclusions and Recommendations

TIME provides the NEB with an effective time management and reporting tool. Updating, reporting and review on a more timely basis are now possible and identification of problems is easier than under the previous system. In addition, the system has enabled new reporting policies to be implemented. While some tardiness in reporting remains, the system supports better overall control and should enable the NEB to base cost-recovery on more current information. Additionally, the accuracy of the data is improved by the more timely reporting and, overall, the quality of the data should be much improved.

The security of the data is at least as good as under the old system. The overall risk of to the integrity of the TIME system and data is minimized by avoiding exposure to the public Internet. There are a number of areas that merit attention but no major weaknesses in processing controls were identified in this audit.

In terms of the design and coding, two fairly serious vulnerabilities have been identified: an SQL-Injection vulnerability; and exposure to Cross-Site scripting attacks. There are also a number of other areas where security could be improved by adjusting the code or by upgrading to a later version of .NET. These are summarized in the text.

All potential vulnerabilities and areas of concern are highlighted in italics in the *Findings* section of the report. The following recommendations, if implemented, will address these potential vulnerabilities and improve the overall security of the system. The recommendations are presented in order of priority.

Recommendation 1: Procedures should be implemented to protect against an SQL-injection attack. As a minimum, input parameters should be validated and parameterized queries should be used.

Recommendation 2: Procedures should be implemented to protect against cross-site scripting attacks. *Server.HTMLEncode* can be used to protect input that is being displayed as part of an HTML page. *Server.UrlEncode* can also be used to protect input that is being used as part of a URL, such as a query string value passed to another Web page. Additionally, the content and length of input can be validated by using the ASP.NET validation controls. Consideration should be given to converting to a .NET 2003 product and deploying this in the TIME application. This would significantly decrease the current cross-scripting attack vulnerabilities.

Recommendation 3: Action should be taken to implement business continuity provisions, particularly the Disaster Recovery Plan, as soon as possible.

Recommendation 4: A Statement of Sensitivity (SOS) of the TIME data should be prepared to provide a basis for ensuring that the data is appropriately protected and handled. All sensitive data should carry sensitivity markings in accordance with the SOS.

Although beyond the specific remit of this audit, it is recommended that a SOS also be developed for the HRIS data.

Recommendation 5: As there have been some changes in personnel responsible for addressing the findings of the TIME TRA, and as it is not clear that all the findings have been addressed, the TRA findings should be reviewed to ensure that all vulnerabilities have been addressed.

Recommendation 6: Procedures should be implemented to ensure that all changes to the TIME system (including non-scheduled maintenance) are documented. Documentation should include the actual script, the time and date that the request was made to run the script, the name of the person requesting that the change be made and the name of the production staff member who applies the change.

Recommendation 7: It is recommended that automated tools be run to help lock down Windows and IIS. It is also recommended that domain controllers be isolated.

Recommendation 8: In order to increase database security, it is recommended SQL Services be run under a low-privilege domain user account. It is also recommended that *xp cmdshell* be removed unless it is absolutely necessary. Lastly, it is recommended that auditing be implemented for SQL (i.e. the SQL Audit level option should be set to *All*.)

Recommendation 9: Consideration should be given to using the built-in authorization features of Windows and specifically the ASP.NET support for role-based authorization.

Recommendation 10: Although the validation methods currently in TIME do not pose a security threat, it is recommended that ASP.NET validator controls be used where deemed appropriate. These controls are very simple to implement and serve as an added measure of defence even if the code logic sufficiently handles validation logic. At the very least, validation controls could help minimize the amount of code required by the server-side validating routines.

Recommendation 11: Although beyond the remit of this audit, it is recommended that a Threat and Risk Assessment be conducted on the Bridge and Human Resources Information Systems.

References

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

2. NEB Policies, Practices and Procedures

2.1 NEB Security policy and procedures, July 2001
2.2 IT Security Audit and Review, TRM Technologies, January 15th 2004.
2.3 TIME V3.0 Help
2.4 TIME Project Charter
2.5 TIME Project Management plan v.3.0
2.6 TIME TRA (Excel Spreadsheet)
2.7 Presentation: TIME TRA Review, 12 January 2004.
2.8 TIME report mock ups (28 files in total)
2.9 TIME report use case (10 files in total)
2.10 SQL Server Backup and Recovery Review
2.11 TIME System Business Rules
2.12 Change Advisory Board Procedures

3. Other documents referenced during the project

3.1 Proposal for the Audit of the Time Information ManagEment (TIME) System, TRM
3.2 Technologies, 17th June 2004
3.3 Action Plan for NEB TIME system audit, August 2004
3.4 Management Planning Guide for Systems Security Auditing, National State Auditors and US General Accounting Office, Dec. 2001
3.5 Site Security Audit Checklist, G Halprin, SysAdmin Group, June 2003
3.6 Computer Security Audit Checklist, C.Rose, ITSecurity.com, April, 2002
3.7 Computer Security Audit Checklist, Chris Hardie, Summersault.com, April 2003

Persons interviewed for this audit

The following NEB staff members were interviewed during this task.

Albert Fung, Manager, Audit & Evaluation
Jeanette Johnston, TIME system administrator
Howard Plato, Team Leader, Desktop and Network
Kevin Campbell, IT Security Coordinator
Mike Knopp, TIME system analyst and programmer
David Young, Team Leader, Information Systems
Elke Meyer, Business Change Analyst, Project Manager of TIME Phase 1