Executive Summary

Audit Objectives

The primary purpose of the audit was to assess the effectiveness and efficiency of security measures and their compliance with Government Security Policy (GSP) and Operational Standards.

The objectives follow Treasury Board's Audit of Security and Audit Guide to Information Technology Security and include the assurances that:

- a management control framework exists;
- an effective security program is in place;
- security education and training is adequate;
- information/communications is appropriately classified and protected;
- an effective personnel screening program is enforced;
- security breaches are dealt with;
- physical safeguards are in place for the protection of personnel and assets;
- contingency management has been developed;
- security requirements are met in contract management; and
- threat and risk assessments are conducted on a regular basis and prior to major system, application and telecommunication changes.

Audit Scope and Approach

The information used in this report was collected through the review of relevant documents, interviews and visual inspections of security measures on site. Interviews were also completed with the user community to obtain their comments and determine their understanding and capability to apply the security practices and standards in their own environment.

The audit team used the audit questionnaires and audit plan developed during the preliminary survey phase and reviewed the management control framework related to the security function.

The following elements were audited:

- Security Management Control Framework
- Administrative Security
- Physical Security
- IT Security

- Personnel Security

Conclusion

We conclude overall that the Councils are taking adequate security measures and, in fact, have made significant progress over the past few years. Nonetheless, there are some existing weaknesses and concerns that still need to be addressed.

As a result of our security audit we provide the following independent opinion in response to the audit objectives specified in the statement of work (Audit terms of reference):

1. **Is there a management control framework?** Although there is an existing management control framework it is not complete and we recommend the development of security accountability, security responsibilities, the completion of the Councils' Security Policy and several other related measures.

2. **Is there an effective security program?** There is an existing and reasonably effective security program currently in place. Recommendations in this report will provide the program with the tools and means to be fully effective.

3. **Is security education and training adequate?** Security education and training is currently not adequate. It is conducted on an ad-hoc basis and is not part of an overall security training and education program.

4. **Is information/communications appropriately classified and protected?** We have made recommendations regarding the appropriate classification of information holdings.

5. **Is there an effective personnel screening program?** The personnel screening program is effective.

6. **Are security breaches dealt with?** Security breaches are dealt with on an ad-hoc basis. We have recommended the development of incident reporting procedures to ensure a common approach and to ensure that incidents are correctly reported and handled.

7. **Are physical safeguards in place for the protection of personnel and assets?** There are effective physical safeguards in place for the protection of personnel and physical assets. We have made recommendations regarding awareness of personnel to potential physical risk situations.

8. **Has contingency management been developed?** Contingency management has not been developed, except for a high-level Y2K Disaster Recovery Plan for IT. A Disaster Recovery Plan is included within the overall Security Plan.

9. **Are security requirements met in contract management?** Security requirements are not completely met in contract management. We have made several recommendations that will ensure compliance.

10. **Are Threat and Risk Assessments (TRAs) up to date and adequate to the need?** Although TRAs have been completed on a regular basis, the recommendations they contain have not always been implemented. We have made several recommendations on this subject.