Canadian Grain Commission
Information Technology Security Review
2003-2004

Executive Summary

This report presents the results of an Information Technology (IT) security inspection that was undertaken for the Canadian Grain Commission (CGC). 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 Treasury Board Secretariat (TBS). This review, which was conducted for the CGC between December 2003 and February 2004 addresses this monitoring and assessment need.

Information technology (IT) is vital to the CGC's operations, and 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. This report provides the CGC 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 is also intended to alert the CGC to existing vulnerabilities and areas of weakness in approach as well as identifying opportunities to strengthen the security posture of the department. (Please note that the focus of this review is limited to practices and procedures required by the Government Security Policy and related operational standards. This review does not include assessment of the specific technical security measures currently used by the CGC.)

The methodology used for this inspection combines a number of techniques. Checklists were used to assess 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). A physical site inspection of IT facilities was also undertaken and interviews were conducted with CGC staff members.

In quantitative terms, 57 policy requirements were examined to assess GSP compliance, and 167 factors were assessed in determining compliance with the related policies and operational standards. 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.

The overall level of compliance with government IT policies was found to be only moderate. In a small number of instances, the deficiencies are quite serious. In particular, the fact that there is no Departmental Security Officer, departmental security policy, IT

security policy or departmental information classification guidelines, is highly irregular and gives grounds for concern. In addition, there are some serious omissions in documented procedures that need to be addressed if future problems are to be avoided.

The report includes 25 conclusions and makes 29 recommendations, including a number that are identified as being of high priority. Implementation of these recommendations will help bring the CGC into much closer alignment with government policy and standards requirements and will strengthen the overall security posture of the CGC.