Report

SYNOPSIS

Audit of Departmental Security Management Control Framework
Project Number 2004-65152
Final report – September 10, 2004

The following is a non-sensitive synopsis of the audit of Departmental Security Management Control Framework. The full report cannot be released due to its security designation level.

Following the events of September 11, 2001, the Government of Canada Security Policy (GSP) was revised and its scope broadened to encompass “safeguarding employees and assets and assuring the continued delivery of services.”

The objective of the audit was to determine the extent to which the Fisheries and Oceans Canada’s (DFO) Security Management Control Framework meets the GSP.

This Security Management Control Framework includes the security organization and associated accountabilities, roles and responsibilities, leadership, planning controlling, administering, training, communication and monitoring activities.

The audit examined the following elements or lines of enquiry:

- management structure;
- policies and procedures;
- planning process and risk management;
- awareness and training;
- breaches and violations; and
- business continuity planning and emergency preparedness.

Key Findings

1. ***Significant improvements have been made to the Security Program since 2002:***

    - A PeopleSoft Security Module has been implemented that facilitates the tracking of employee security status;
    - Improvements to the efficiency of the security clearance process;
    - Major enhancements to departmental security communications;
    - The development of a comprehensive security function accountability framework;
    - The development and delivery of a one-day security training course; and
    - Significant improvements made to the DFO Business Continuity Planning Program.

The audit concluded, however, that in spite of these initiatives which have strengthened the departmental security program, there remain weaknesses that expose the department and its employees to unnecessary risk.

The Headquarters and regional organizational structure linking the Occupational Health and Safety (OHS) function with the Security function enhances the effectiveness and efficiency of carrying out these functions…………………(Section 16 (2) (c) of ATIA)

2. Communication With Senior Management

The job description for the DSO describes a “dotted“ line relationship between the DSO and the DM whereby the DSO has a recognized direct access to the DM if the situation warrants. This access, which transcends the organizational line reporting relationships, is important given the sometimes sensitive and urgent nature of security issues, and the fact that the DM is ultimately accountable for security in the Department.

3. Security Accountability Framework

The department has made an excellent start in identifying the full scope of its security activities.

HQ Safety and Security Branch has developed an accountability framework that identifies all significant activities associated with Security, Business Continuity Planning (BCP) and Emergency Preparedness. The framework details the roles and responsibilities of the national HQ security organization, the regional security organization and sector/site management.

The audit concluded that this framework is an excellent tool to clarify the full range of important activities within the DSO mandate.

4. Senior Management Oversight of the Security Function

There has been a lack of senior management oversight of security.

The audit found that significant security issues are not regularly made known to the DMC. During Fiscal Year 2003/04, for example, security related issues have been on the DMC agenda only three times, and in all three instances the issue related to resourcing requirements.

5. Communication Between the HQ Safety and Security Branch and Regions

The audit concluded that communication between the HQ Safety and Security Branch and its regional counterparts has been insufficient to ensure adequate coordination of the DFO Security Program. Teleconferences including HQ and the Regions have occurred on an infrequent basis. As a result, RSOs are not sufficiently aware of HQ’s planned activities, nor is HQ adequately informed of the issues and initiatives at the regional level.

6. Integration of Departmental Security Initiatives with Information Technology Security

The Information Management and Information Technology (IM-IT) Directorate of DFO has a small dedicated IT Security Unit comprised of two FTEs. This Unit has the responsibility for identifying IT security requirements in the Department…………(Section 16 (2) (c) ATIA)

7. Coordination of Security Initiatives with Sector Management

The audit noted that the only national security network in DFO is the network of RSOs linked to the DSO and his staff…………….(Section 16 (2) (c) ATIA)

It is important that the DSO at the national level and the RSOs regionally have the capability to contact and inform departmental field staff of issues and policies pertaining to security, as well as to be informed of security incidents that arise in the field.

8. Resourcing of the Headquarters Security Function

Emerging security demands may soon put pressure on resource levels at Headquarters.

The DMC decision in April 2002 to increase the resource commitment to the HQ security function by $1.6 million recognized the importance of achieving strong corporate governance, national services, policy development and program monitoring.

9. (Section 16 (2) (c) ATIA)

10. Accountability For Security Related Resource Allocations

The audit concluded that resource challenges at the level of regional security operations have been compounded by insufficient accountability for resource allocations specifically directed to the security function.

The Acting Departmental Security Officer has acknowledged the accuracy of the audit report and has defined an aggressive program of corrective initiatives.

Major activities include:

- The development of Safety and Security Policy and Accountability Framework prepared November 3rd, 2004;
- The development and review of an updated Threat & Risk Assessment methodology for the Department;
- The development of a Project Management methodology to track the implementation of the recommendations in the audit report;
- The development of a dashboard methodology with which to brief senior management and report the status of security implementation.