National Defence / Défense nationale

Chief Review Services

REVIEW OF DND/CF INFORMATION SECURITY

October 2002

7050-7 (CRS)

Canada

TABLE OF CONTENTS

SYNOPSIS

This report presents the abbreviated results of a review of Information Security within the Department of National Defence and the Canadian Forces (DND/CF). The review, conducted with the support of a team from KPMG Consulting, was largely interview based and included an assessment of DND/CF organizational structures, policies and practices relative to leading information security practices followed by other organizations. The report also benefited from a concurrent review of departmental compliance with the Government Security Policy (report is on the CRS Internet site).

The review encountered changing circumstances within the DND/CF and, in many aspects, has served to document the perspectives, as well as corresponding initiatives, of management. (It also offers a graphically-depicted baseline assessment as at February 2001). Principal among the changes being implemented in the latter stages of this review, was the creation of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) and the assignment of Information Management to the head of that Office, the Associate Deputy Minister. This, along with the recently created Directorate of Information Management Security (D IM Secur), in the Information Management Group, has introduced structures which will support attention to the recommendations of this review. The requirement for a central focal point for information security matters formed a key recommendation of this review.

Understandably, origins in the policing function will have contributed to observed rigidity in information security policies. At the same time, Security Operations' initiatives have equally contributed to the advanced state of current information security monitoring tools and techniques. It is also noted that since the review, an advanced Test and Development Centre has been established in the DND/CF to manage external connectivity.

The comprehensive management action plan forms a key part of this report and appears in Annex A. Among the many initiatives are those to: staff the Directorate of Information Management Security; revise the information security policy framework; and, introduce an interim awareness program.

It is recognized that the management action plan, prepared in response to the recommendations in this report, will have resource implications for the organizations involved. These implications should be considered as part of the normal business planning process.

This review was conducted as part of the approved Branch Work Plan. The review conclusions do not have the weight of an audit and must not be regarded as such. While sufficient to enable the development of recommendations for consideration by management, the assessments provided, and conclusions rendered, are not based on the rigorous inquiry and evidence required of an audit. Accordingly, they are not represented as such, and the report reader is cautioned.

OVERVIEW

INTRODUCTION

1. As part of the 2000/01 review plan, Chief Review Services (CRS) assessed DND/CF information security practices for relevance, currency and appropriateness, especially in terms of risk management. This review was conducted during the period September 2000 – March 2001.

2. The aim of the review was to provide senior departmental management with findings, analysis, and recommendations regarding Information Security. The review included research on leading practices within other large organizations.

Comparative Assessment of the DND/CF Information Security Program

3. U.S. Government Experience. A May 1998 publication, *Learning From Leading Organizations,* by the General Accounting Office (GAO) in the U.S., focussed on Information Security Management. It reviewed the practices of eight leading non-federal organizations recognized as having strong information security programs. The top five practices focussed on: recognizing information resources as critical assets; developing practical risk assessment procedures; holding program and business managers accountable; continual risk management; and, designating a central group to carry out key activities such as policy development, user education and program monitoring. While the DND/CF program includes elements of each of these leading practices, some areas require refinement/enhancement.

4. Graphic Depiction of Assessment. As indicated in the summary rating graph at the end of this section (see page 4), our assessment of the DND/CF information security program ranged from "Undeveloped" to "Advanced Practice". This review addressed the following seven components of information security: 1) security organization; 2) policy, procedures and guidelines; 3) security training and awareness; 4) risk management; 5) security operations; 6) security implementation; and 7) critical infrastructure. Critical areas such as overall direction, policies, as well as training and awareness require attention. Other areas were generally representative of good management practice.

5. Risk Management. In general, risk management practices regarding information security are improving, but remain constrained by resource limitations and the ever-constant operational pressures to "get the job done". The DND/CF is also on the cusp of a change from a rule-based security approach, to a risk-managed approach. Current security practitioners are striving to make security requirements more appropriate to the known risks, and to increase the involvement of functional managers in risk management processes and trade-offs.

6. Organizational Focal Point. We concluded that the main area of concern is the need for a distinct and specific departmental office of primary interest (OPI) for information security, which would also be responsible for related policies, training, awareness and monitoring. While other agencies have also had some difficulty in this regard, most have evolved, or are evolving, to the United States Department of Defense (DoD)/Defense Information Systems Agency (DISA) approach, in which information security has become a "corporate" IM responsibility, but with increased delegation to operational or functional managers for program implementation.

7. **NOTE:** During the course of the completion of this review, effective 1 October 2001, the DND/CF established a central focal point for information security matters, the Directorate of Information Management Security (D IM Secur), under the Director General Information Management Operations (DGIMO), in the Information Management Group. At the same time, we recognized that information security is but one, albeit important, element of DND/CF security. Security at the departmental level should co-ordinate and integrate several aspects, including personnel, physical, information and administrative/operational considerations. This represents a major challenge for the incumbent Departmental Security Officer (DSO), DPM Secur, reporting to the CF Provost Marshall. In view of the importance of the function and responsibilities, our view is that there may well be merit in addressing the seniority and visibility of this position.

RECOMMENDATIONS

The following recommendations resulted from our review and assessment.

Establish an Information Security Central Focal Point

8. The GAO has identified the establishment of a central focal point for information security as a leading practice with responsibility for coordinating common initiatives, assessing risk, establishing and maintaining policies and a central information security plan, promoting awareness, and monitoring information security. This central focal point also helps to optimize the allocation and use of security resources.

9. This has been actioned in the DND/CF. Now that the information security central focal point has been established in the DND/CF (D IM Secur in the Information Management Group), the remaining key recommendations can be implemented.

Formalize and Standardize the Creation of Policies

10. Information security policies require significant improvement to be effective. Related policies should include all aspects of information, both manual and automated (i.e., information handling and information technology). They should be divided into two broad segments: concise high-level directives and more detailed procedures. Policies should be developed by D IM Secur, while procedures would be the responsibility of local units. Although the breakdown between policy and procedure already exists in some units, the key to this recommendation is to formalize and standardize this process and complement it with a monitoring function performed by D IM Secur.

Develop a Training and Awareness Program

11. The current DND/CF information security training and awareness program is neither structured nor formalized. Improved employee training is required to reduce the probability and severity of security incidents or breaches. Failure to fully address training and awareness issues can limit the effective use of new technology within the DND/CF. D IM Secur should be responsible for coordinating the program. Ongoing awareness briefings should also be developed for senior management in this regard.

Adopt a Risk Management Framework

12. Significant changes to the expected degree of connectivity for departmental information systems have greatly increased the inherent threats and risks. This evolving technological environment also brings about changes in the way organizations must manage risk. They can no longer afford to maintain the old risk avoidance or rule-based approach to information security. For example, instead of trying to protect all of its information, the DND/CF should consider focussing its efforts on the most critical information. As practiced by DoD, 80 percent of available resources could be used to protect the core or critical 20 percent of information, while the remaining information can be more openly shared. Risk must be accepted at lower levels within the organization to promote accountability and in order for such a strategy to work effectively. This will require an increased degree of formalization and documentation of risk management to contribute to an improved risk management framework.

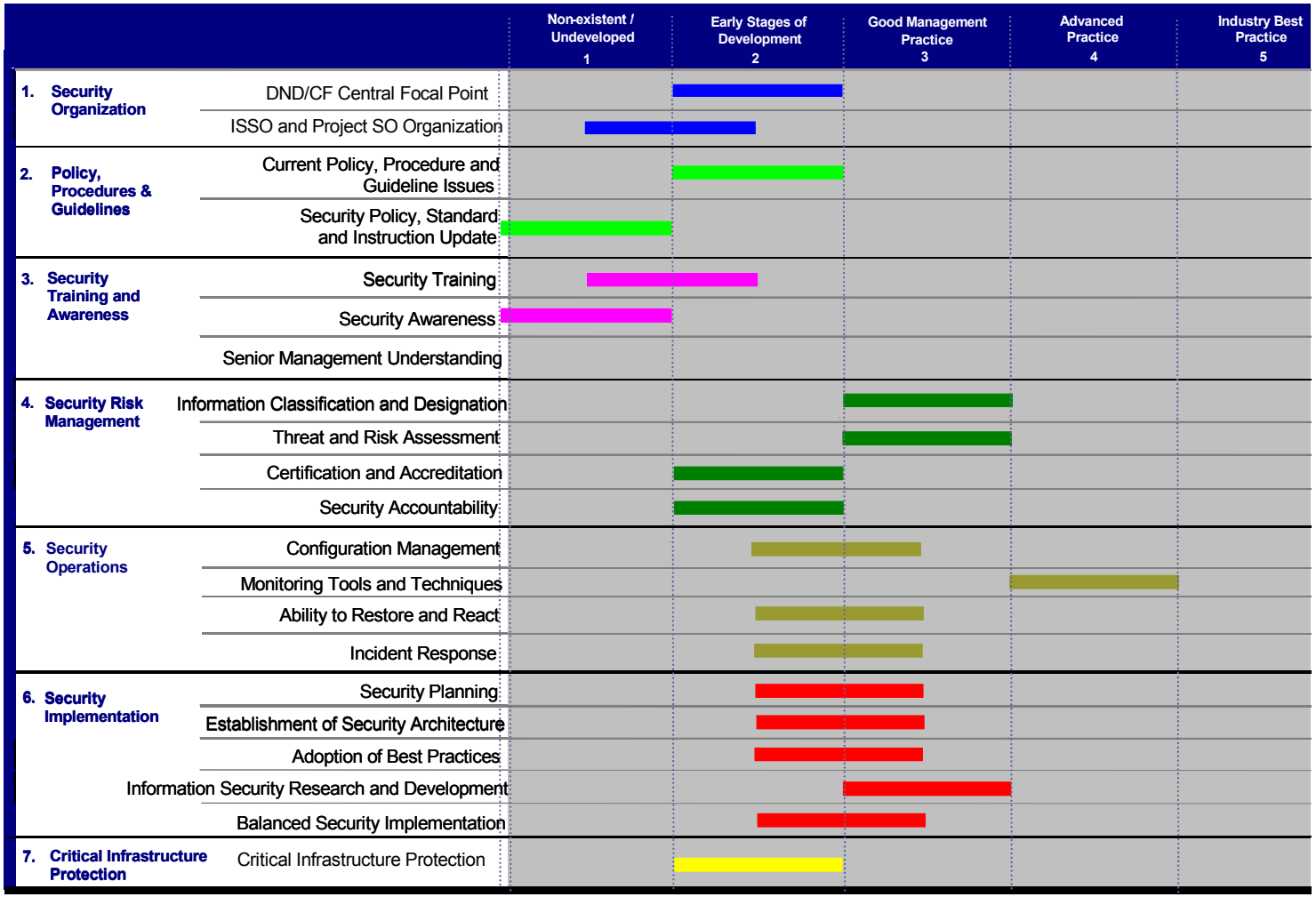
Update the Information Security Architecture

13. At the time of our review (September 2000), the consensus of those interviewed in the IT community (40-50 senior IT personnel) was that the security architecture at that time was not up-to-date, although some were aware that initiatives to improve it were underway. We understand that while the new security architecture is not yet official, it is in implementation. Care should be taken to formalize and document this new security architecture with appropriate approvals.

Critical Infrastructure

14. Many of the issues facing the new Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) are similar to those analyzed in this security review, only on a larger scale. The role of the new office is to provide a focal point for the federal government's cyber incident analysis and coordination efforts and to support federal departments and agencies in meeting their security responsibilities. Accordingly, D IM Secur activities should be closely coordinated with those of the OCIPEP. This synchronization of security efforts will ensure the consistent application of scarce resources and leading practices, and the continual enhancement of security operations.

Management of Information Security - Summary Rating Graph as at February 2001



ANNEX A

MANAGEMENT ACTION PLAN

Part I – Information Security Organization

1. ADM(IM), under DGIMO, initially established the Directorate of Information Management Security (D IM Secur) effective 1 October 2001. Since October 2001, the D IM Secur establishment has been finalized and includes six elements:

a. D IM Secur Coord Section – Business Planning, Document Library and Administrative Support;

b. D IM Secur 2 Section – IM Security Policy, Training & Awareness, IM systems Certification & Accreditation, and Verification and Audit services;

c. D IM Secur 3 Section – Designated Domain Security Management, including PKI Service Management (Designated);

d. D IM Secur 4 Section – Classified Domain Security Management, separated into Secret and below and Top Secret and above, as well as classified PKI Service Management (Classified);

e. D IM Secur 5 Section – IM Security Program management, including IM Security Plans, requirements and standards (international and national); and

f. CFCSU – DND/CF Crypto support including management of the CCKEMS key management system.

2. Many positions remain vacant, however, there are a number of parallel efforts ongoing to staff civilian positions ranging from the Director to several CS 02 INFOSEC professional positions throughout the directorate. These actions have been ongoing in earnest since December 2001. DGIMO has designated D IM Secur as a top priority for manning/staffing for 2002/03 and 2003/04. It is anticipated that the D IM Secur transition will be completed and 80 percent manned by **September 2003**.

ANNEX A

Part II – Information Security Policies, Procedures and Guidelines

3. D IM Secur and D PM Secur are in the process of revising the information security policy framework. This framework, to include authorities, documentation structure, review frequency and information dissemination means, is an essential first step to improving the information security policies in the DND/CF. D PM Secur has agreed to have D IM Secur draft, revise and maintain the key National Defence Security Instructions (NDSI) chapters as they pertain to information security (i.e., Chapters 70 and 71), and a new sub-section has been established in D IM Secur to focus on Policy, Training and Awareness. This work will require a continuous cycle of review, revision, publishing and dissemination over **the next two years** and is resource dependent.

4. D IM Secur already has a DND Intranet web presence with links to other information security information sources and sites, however, a consolidation and rationalization effort, as well as inclusion of a proper information resource library on-line has not yet been established. The information structure of the D IM Secur web site will be reviewed over the period **September – December 2002** and a plan devised to revise it to provide clear access to INFOSEC policies, training resources, procedures, guidelines, standards and instructions. This will also need to be replicated in all information domains (i.e., designated and classified). A phased implementation of an information security web portal is planned over the period **January – September 2003**, as resources permit.

Part III – Information Security Training and Awareness

5. D IM Secur, and formerly the IPC, has taken responsibility for training and awareness of information security professionals and members of the CF by initiating and staffing both an awareness program and training series of OSQs and OSSs. This staffing action is progressing well with detailed work ongoing between D IM Secur and ADM(HR-Mil) staffs in both areas, however, this solution will meet the DND/CF longer-term requirements **from 2003/04 onwards**.

6. In the interim, D IM Secur is investigating implementation of an interim awareness program, based on existing ones in other Government departments and allies, to address the short-term requirement to take the Department up to the point where the formal training and awareness program has been established. Both of these actions will carry on in parallel, resource dependent, with priority given to the longer-term program for training and awareness. Coordination with related trade structure reviews, such as MOSART, will be undertaken as part of this effort as well as the creation and validation of detailed OSQ and OSS and training plans. This is ongoing and an interim awareness program is planned to be in place by **November 2002**.

ANNEX A

Part IV – Information Security Risk Management

7. It is well recognized that the existing Certification and Accreditation process is cumbersome and needlessly complex for the vast majority of information systems. D IM Secur staff, in coordination across the matrix and information security stakeholders, has been engaged in revising the current C&A process to both rationalize and synchronize the existing configuration control mechanisms, such as the Request for Change (RFC) process under the national IM Configuration Control Boards since July 2001. It is the intent of D IM Secur to scale the C&A requirements to the value and sensitivity of the information (and information system) being accredited. This is similar to the processes used in the US DoD. It is also intended to use as much documentation as practical from other processes (i.e., Project documentation, System Architecture, CONOPS, etc) in order to reduce the level of duplication. D IM Secur has already modified the final accreditation documentation to reflect a more direct risk management approach by including system managers and system technical authorities in the accountability chain prior to final acceptance of risk by the designated operational authority. In one case, the conditions of accreditation for one large tactical information system were translated into specific direction throughout an environmental command and other stakeholders. The C&A Process Revision will be continuous, but an initial revision is planned to be completed by **December 2002**, resources dependent.

8. It should be noted that while the CRS report recommends acceptance of risk at lower levels within the organization to promote accountability, this is actually in contrast to the trend towards greater and greater interconnectivity of systems, therefore leading towards the tendency for actual risk to be incurred at higher and higher levels. For example, while it may make sense for a commander in a deployed operation to accept the risks resident in having access to a national command and control or intelligence system locally, the actual risk to those information holdings or systems is incurred at a much higher level due to the connectivity and relative ease that any user (authorized or not) can access a wide variety of information not constrained to that theatre of operation.

Part V – Information Security Operations

9. Configuration of national systems, both classified and designated or unclassified, is managed through the associated Configuration Control Boards (IM CCBs) under DGIMO. D IM Secur sits as a Core Advisor on both the Designated and Classified CCBs. This activity is highly resource and time intensive and many of the tools that would enable a more disciplined approach to configuration control are not yet in place. DDCEI has been given the lead within DGIMO to revise the CCB processes.

ANNEX A

10. D IM Secur and CFIOG, with assistance by DMR, have developed a detailed Information System Security Incident Handling (ISSIH) process for application at the national to site levels. This process incorporates the CF Network Operations Centre (CFNOC), which was established on 3 September 2002 at CFS Leitrim by combining existing network management and computer security teams. The ISSIH process and procedures have been been disseminated widely across the DND/CF.

11. D IM Secur and CFNOC will review current network vulnerability assessment capabilities and procedures with a view to ensuring that higher risk/high sensitivity systems are assessed as a first priority. This area requires significant resources both in terms of depth and breadth of skills.

Part VI – Security Implementation for IT Projects

12. The DND Information Technology Security Architecture was last rewritten in August 2000, and was not formalized or promulgated in an official manner. This document, although still largely current and relevant, will be revised and updated to reflect work done since in the areas of wireless systems security, connectivity to contractors, separation of the Designated and Classified infrastructures, the General Purpose Network (GPNet), the Top Secret networks, laptop security, new options for security at the network layer, deployment of Intrusion Detection Systems (IDS), Trusted Guards, defense against malicious code and others. The resulting document will be staffed for approval and promulgation through D IM Secur by **September 2003**.

13. In addition to continued guidance and direction to projects on all aspects of IT security, a number of project independent initiatives are actively being pursued to contribute to the implementation of the IT Security Architecture. An enterprise capability to protect against specific and focused malicious code attacks is being investigated and procurement activity will be initiated in **FY 2002/03**. A great deal of emphasis is being placed on the security requirements to interconnect entire security domains that have traditionally been kept separate for security reasons. A firewall support team and a supporting engineer position will be staffed by **August 2003** in order to focus on the proper implementation of security solutions in this area, and policy has been drafted to ensure that the interconnection of security domains is a centrally controlled activity. Efforts to identify mechanisms to enforce the security posture and configuration of DND workstations and servers will continue, with a way ahead identified **by August 2003**. Finally, enterprise-wide security policies for the implementation of common infrastructure, such as a common Network Operating System (NOS) and common directory services, will be developed and coordinated as new technologies are rolled out **over the next few years**. A host of smaller initiatives are also aimed at filling in the security gaps that currently exist in the implemented infrastructure.

ANNEX A

Additional Action Areas:

14. Enhance IS Security support to operations. D IM Secur will further define and implement IS Security management and support structures to include roles, responsibilities, accountabilities and reporting procedures for ISSOs, System managers, etc. This is planned to be completed by **December 2002**.

15. Define and Foster Key partnerships. D IM Secur will establish and enhance key partnerships with OCIPEP, CSE, DFAIT, D PM Secur, PCO, NATO, CCEB and other agencies and organizations over the ensuing six to 18 months **(August 2002 – January 2004)**.

16. Establish a standards and requirements capability. D IM Secur will establish a standards and requirements capability to support IT projects in defining their security requirements. This will not replace the larger requirements process, but is meant to address the lack of clear guidance in some areas of security standards when implementing IT projects. This capability is partly in place, but highly dependent on resource allocations and will be subordinate to the requirements definition surrounding crypto modernization. It is planned to have this capability in place by **September 2003**.