National Défense
Defence nationale

Chief Review Services

REVIEW OF DND/CF COMPLIANCE WITH THE GOVERNMENT SECURITY POLICY – A UNIT PERSPECTIVE

April 2002

7050-7 (CRS)

Final Version 11 April 2002

Canada

SYNOPSIS

This report presents the results of a review, conducted in partnership with KPMG Consulting, to gauge DND/CF compliance with the Government Security Policy (GSP). The focus was at the local/unit level; upwards of 20 locations were visited in 2000. This unit-level "snapshot" provides a reasonable, albeit not definitive, view of DND/CF compliance with the GSP. While the review did consider aspects of Information Security, a more targeted review of that subject was carried out concurrently and is being reported under separate cover.

The review found instances of non-compliance and partial compliance; corresponding recommendations for improvement have been made. Areas requiring the most attention were the awareness and testing of local emergency and contingency management plans. IT security monitoring processes also require updating and an improved risk-management orientation.

Notwithstanding the above, overall unit-level compliance with the GSP was found to be satisfactory. This conclusion is reinforced by the prompt action and detailed plans provided by the Deputy Provost Marshall – Security relative to the matters raised by the review. At the same time, it is important to recognize that the assessment was completed prior to recent events which have significantly raised the bar with respect to security requirements. Accordingly, additional targeted review work is underway. It is also noteworthy that the GSP is currently undergoing amendment and any significant changes will ultimately have to be addressed through such action plans.

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.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

OBJECTIVE & SCOPE

The principal objective of this review was to assess DND/CF local/unit-level compliance with the Government Security Policy (GSP) promulgated by the Treasury Board (TB).

The seven main areas addressed are as follows:

- Security Organization;
- Security Administration;
- Physical Security;
- Personnel Security;
- Contingency Management;
- Contract Management; and
- Information Technology Security.

The field work was conducted in 2000. It was performed at more than 20 unit locations identified through a combination of random and judgmental selection.

Weapons security, and the security of other sensitive inventories were not included in the scope.

SUMMARY OF RESULTS

In general, we found the DND/CF security program to be compliant with the GSP. There are areas requiring improvement, however, we have not judged them to be so significant as to qualify the overall rating of "compliant".

Indications of the degree of compliance, along with the key recommendations and responsible organizations are presented in the 1-page chart which follows. Subsequently, the detailed results, assessments and recommendations appear in the KPMG slide package which has been incorporated into this report. Finally, details of corrective actions taken and planned are presented at the end of this report.

CHART 1
DND/CF Compliance with the GSP - Compliance Rating and Recommendation Summary

Topic Area	Rating	Focus of Key Recommendations	OPI/OCI
1. Security Organization	Compliant	Re-emphasize role and responsibilities of Departmental Security Officer (DSO)	DPM Secur[1]
		Security reviews/inspections should be formalized	"
		Unit Security Officer (USO) roles should be standardized	"
		Security training and awareness programs should be strengthened	"
2. Security Administration	Compliant	Policies and guidelines for information classification should be simplified and standardized	DSO[2]
		Threat and Risk Assessment (TRA) processes require improvement	DPM Secur
3. Physical Security	Compliant	Regular security reviews are required at the unit level	DPM Secur
		Records management requires standardization across all units	DSO
4. Personnel Security	Compliant	Employee screening and release procedures should be improved	DSO and HR OPIs[3]
5. Contingencies and Contracting	Partially Compliant	Unit personnel should be made aware of contingency plans	DSO
		Contingency plans should be tested regularly	DSO
		Contractual security issues should be included in policy documents	DPM Secur
6. Information Technology Security	Partially Compliant	Security issues should be addressed in all planning initiatives	DSO
		IT security monitoring and review should be established	DPM Secur
		IT certification and accreditation processes require improvement	& CFIOG[4]

[1] DPM Secur – Deputy Provost Marshall Security
[2] DSO – Departmental Security Officer
[3] HR OPIs – Human Resources Offices of Principal Interest
[4] CFIOG – Canadian Forces Information Operations Group

INTRODUCTION

BACKGROUND

The Government Security Policy (GSP) provides federal departments with a security baseline with which organizations must comply. The Policy does, however, take into account diverging departmental priorities, budgets, and specific organizational culture by defining broad requirements to ensure a certain minimum level of security within a department, as well as government-wide.

The Deputy Provost Marshall Security (DPM Secur), under Vice-Chief of the Defence Staff (VCDS), and the Canadian Forces Information Operations Group (CFIOG), under Assistant Deputy Minister Information Management (ADM(IM)), are the two major organizations most directly concerned with GSP-related matters in the DND/CF.

The GSP guidelines also provide federal government departments with direction and guidance in carrying out self-assessments and reviews of their departmental security programs.

This review is further to a preliminary assessment of GSP compliance carried out by DPM Secur in February 2000.

OBJECTIVE AND SCOPE

The objective of this review was to assess DND/CF compliance with the GSP and operational standards published by TB.

The review focused on GSP compliance at the unit level. The review did not include the security of weapons and ammunition, and other sensitive inventories[5], which are being addressed separately.

APPROACH

Initial Interviews

Compliance issues and expectations were discussed with appropriate TB authorities. Contacts were established with key departmental stakeholders and initial interviews were conducted. Information obtained from these interviews and pertinent TB publications was used as input to the review plan. The intent was to establish an appropriate compliance assessment checklist and a list of key issues to be considered during the review.

The review was divided into the following seven main sections or areas, to correspond to the GSP policy structure and related guidelines:

[5] Items which if lost, damaged, or misused, have the potential to negatively impact the operational capabilities of the CF, to put the safety of the general public at risk, or to affect technology sharing arrangements with Canada's allies.

- Security Organization;
- Security Administration;
- Physical Security;
- Personnel Security;
- Contingency Management;
- Contracting Management; and
- Information Technology Security.

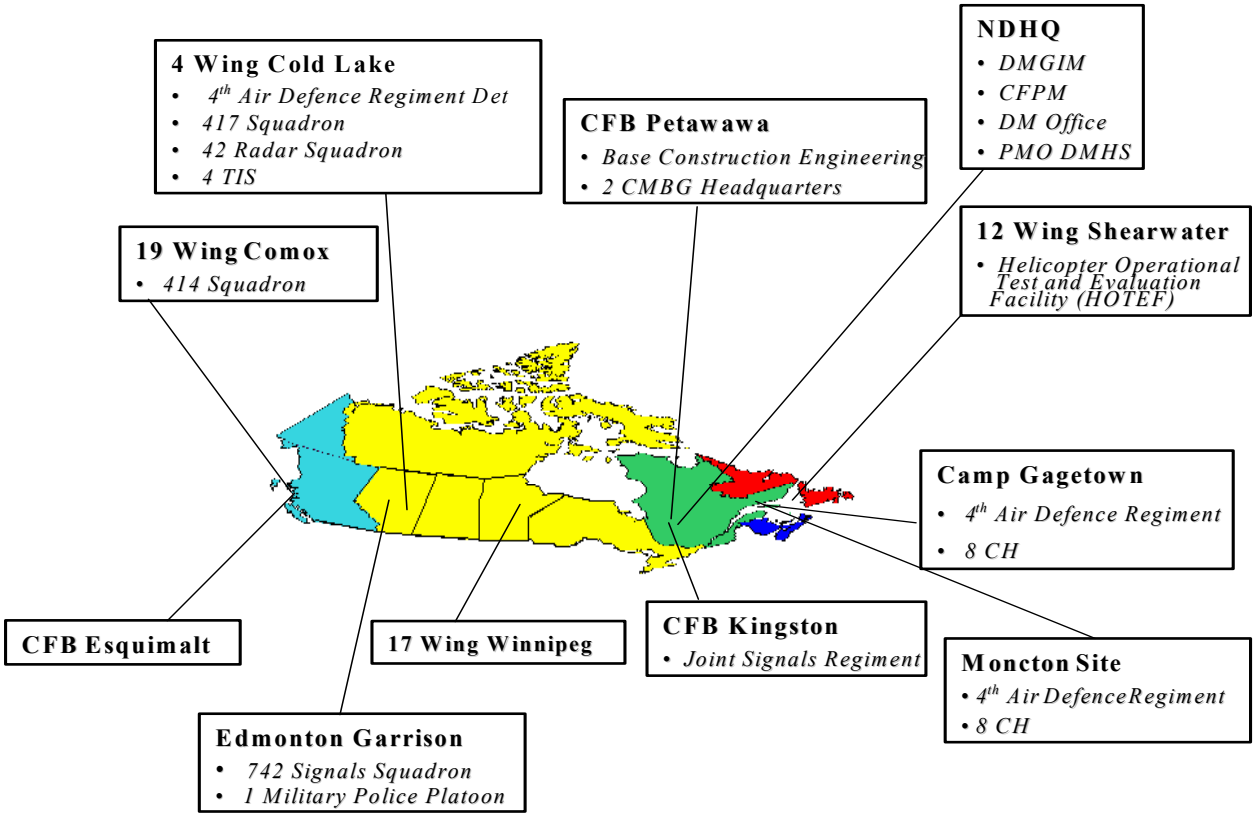
Preliminary Assessment

The results of a DPM Secur preliminary assessment of GSP compliance (February 2000) were considered in this review. In particular, information from the DPM Secur assessment was used to develop a compliance assessment checklist.

Unit Visits

The compliance assessment checklist was used in conjunction with visits to units throughout DND/CF. In order to be as representative as possible, these units were selected on both a random and judgemental basis. As a unit is the main operational element in both DND and the CF, these unit assessments were important in determining overall compliance strengths and weaknesses in DND/CF. As indicated in Figure 1, more than 20 DND/CF units across Canada were included in the review.

Figure 1 - Field Audit Locations



Coverage Period

This review considered the period up until the end of March 2001. All of the interviews and unit visits were conducted during the last two quarters of 2000.

Review of DND/CF Information Security

This review was managed separately from a concurrent Chief Review Services (CRS) review of DND/CF Information Security, but the two projects were aligned to ensure consistency and resource efficiency. A separate report is being prepared for the Information Security Review.

KPMG SLIDE PACKAGE

Government Security Policy Compliance Review

November 2001

KPMG Consulting

Contents

- Introduction
- Organizing Security
- Administering Security
- Physical Security
- Personnel Security
- Security and Contingency Mgt
- Security and Contracting Mgt
- IT Security
- Conclusion

1.1 Background and Purpose

- The Treasury Board Government Security Policy (GSP) is aimed at providing federal departments with high-level policy guidance.
- The GSP takes into account diverging departmental priorities, budgets, and specific organizational culture. It does so by defining broad requirements to ensure a certain level of security within a department or government-wide.
- CRS staff worked with a KPMG team to conduct a review of DND/CF compliance with the GSP.

1.2 Objectives

The CRS/KPMG review had three main objectives:

- Evaluate departmental level of compliance with Security Policy operational standards.
- Determine DND/CF's effectiveness in implementing Security Policy operational standards.
- Ascertain departmental efficiency in implementing Security Policy operational standards.

1.3 Approach and Methodology

- *Aim*: The overall aim of the review was to establish DND/CF compliance with the Treasury Board Government Security Policy (GSP).
- *Scope*: The review addressed a number of DND/CF organizations and units as well as external agencies, the current and planned DND Security Policy Program, the National Defence Security Policy (NDSP) and all related policies, standards and guidelines. The scope did not include the security of weapons and ammunition & other sensitive inventories.
- *Key Issues*: Confirm/validate the DPM Secur preliminary assessment of GSP compliance.
- *Techniques*: This review was conducted using interviews, document review, best practices, research and visits to selected units.

1.4 Unit Visits

- Introduction
- Organizing Security
- Administering Security
- Physical Security
- Personnel Security
- Security and Contingency Mgt
- Security and Contracting Mgt
- IT Security
- Conclusion

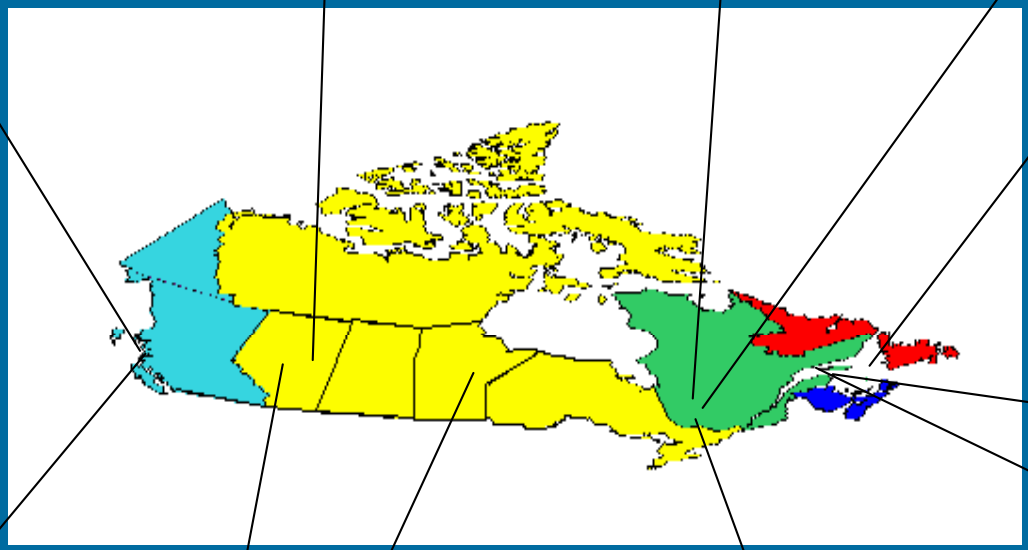
4 Wing Cold Lake
- *4th Air Defence Regiment Det*
- *417 Squadron*
- *42 Radar Squadron*
- *4 TIS*

CFB Petawawa
- *Base Construction Engineering*
- *2 CMBG Headquarters*

NDHQ
- *DMGIM*
- *CFPM*
- *DM Office*
- *PMO DMHS*

19 Wing Comox
- *414 Squadron*

12 Wing Shearwater
- *Helicopter Operational Test and Evaluation Facility (HOTEF)*



Camp Gagetown
- *4th Air Defence Regiment*
- *8 CH*

CFB Esquimalt

17 Wing Winnipeg

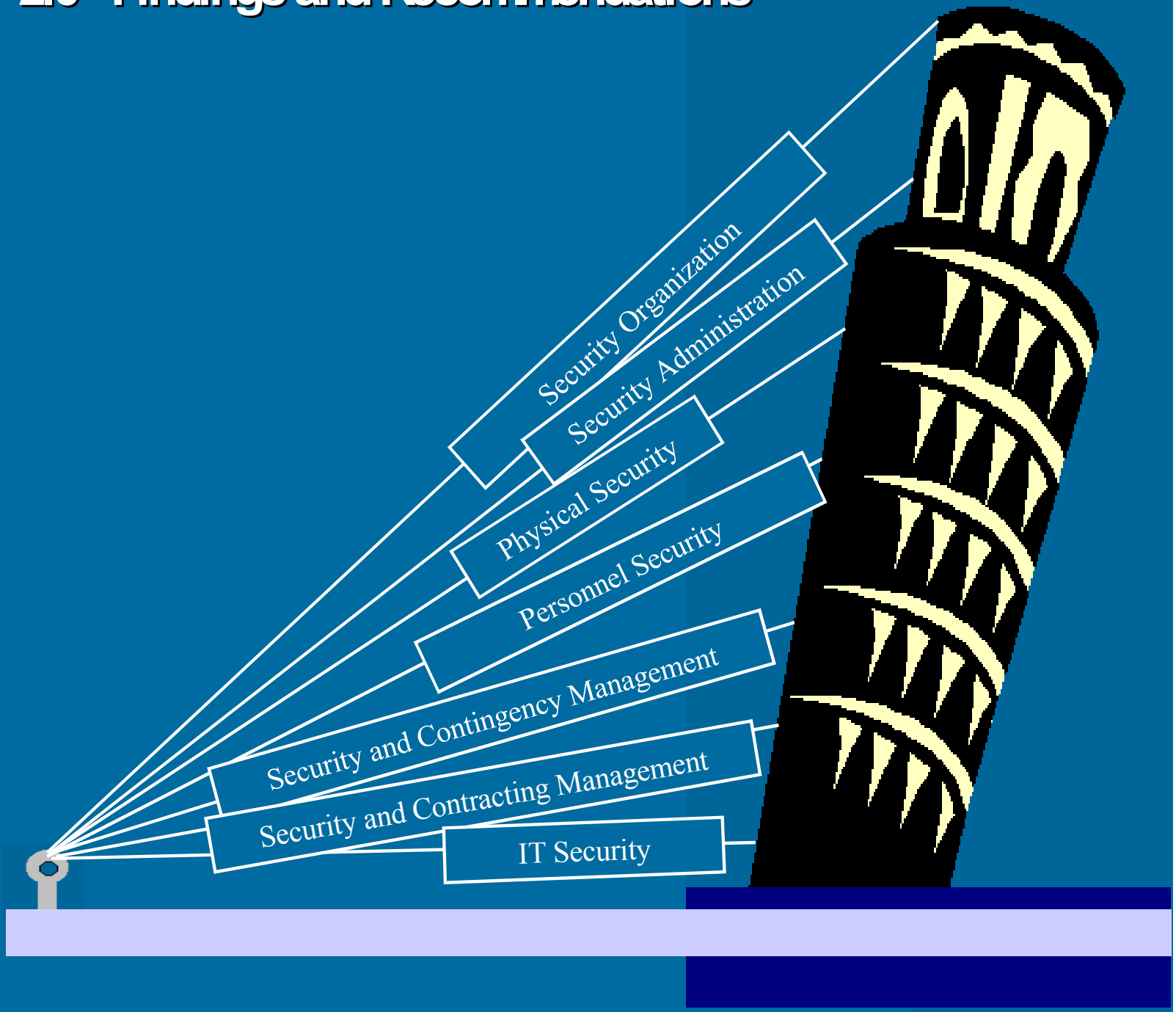
CFB Kingston
- *Joint Signals Regiment*

Moncton Site
- *4th Air Defence Regiment*
- *8 CH*

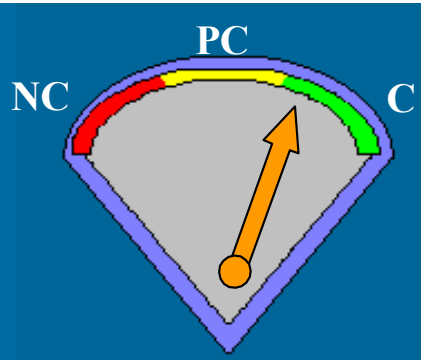
Edmonton Garrison
- *742 Signals Squadron*
- *1 Military Police Platoon*

2.0 Findings and Recommendations

- Introduction
- Organizing Security
- Administering Security
- Physical Security
- Personnel Security
- Security and Contingency Mgt
- Security and Contracting Mgt
- IT Security
- Conclusion



2.1 Organizing Security



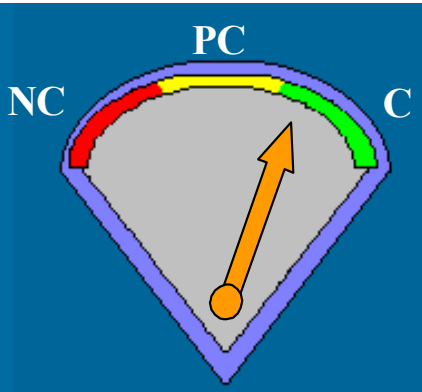
Key Findings

- There is no central focal point.
- The majority of units have local security policies and procedures that are accessible and understandable, but are not necessarily up-to-date or consistent across the units.
- Capabilities, accountabilities, responsibilities, and duties vary among security officers. The ISSO position is not formalized.
- The majority of units are not conducting regular security inspections.
- There is a lack of training and awareness in the department.

Key Recommendations

- Although the current organization structure is compliant with the GSP, gains in efficiency and effectiveness can be achieved with a re-organization.
- The DSO needs to ensure consistency among local policies and security orders with standard security minimums.
- DSO needs to ensure units conduct security reviews/inspections and report results.
- DPM Secur and CFIOG need to standardize USO and ISSO roles and responsibilities across the board. These need to be recognized by management.
- Training and awareness programs should be developed.

2.2 Administering Security

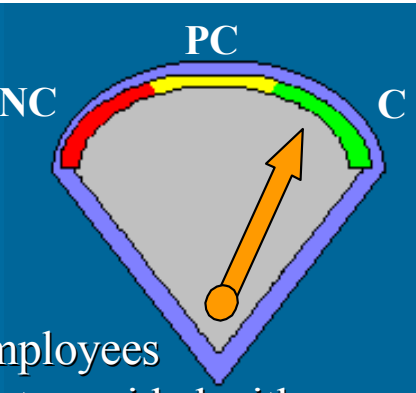


Key Findings

- Information is generally appropriately classified and designated.
- In a number of units, Threat and Risk Assessments (TRAs) are not performed in a timely fashion due to a confusion over who is responsible for their completion.
- Recommendations from recent security reviews/ surveys have been/are being implemented.
- Security infractions and violations are uncommon.

Key Recommendations

- Policies and guidelines for information classification should be simplified and standardized across the Department. In an attempt to reduce the occurrence of over classification, a qualified individual within each unit should oversee information classification. Declassification and downgrading of information should also be conducted on a standard basis, as defined by the DSO.
- TRA templates and training should be provided.



2.3 Physical Security

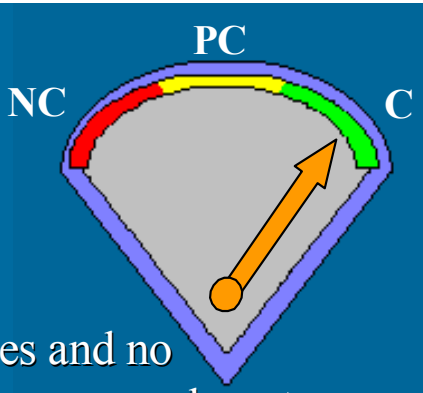
Key Findings

- Very few incidents involving the physical safety of employees have been reported in the past two years. USOs are not provided with copies of incident reports.
- Monitoring and review of security measures is not occurring consistently in all units (e.g., "State of Security" reports).
- The majority of observed units use a local stand-alone Records Management System (RMS).
- The majority of observed units have limited control over sensitive assets.

Key Recommendations

- USOs should be provided with copies of all security incident reports.
- Lack of reporting prevents thorough review to ensure compliance. It also prevents corrective action once breaches are identified.
- A standard RMS should be implemented across all units to ensure documents are properly filed and classified.
- Mobile assets should require sign-in/sign-out privileges.

2.4 Personnel Security



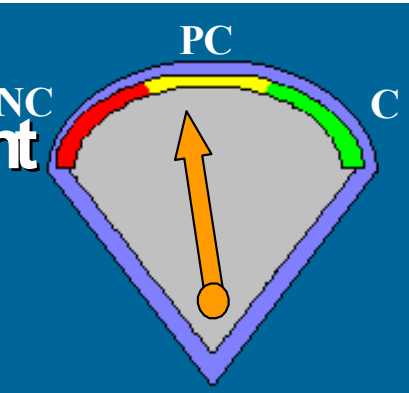
Key Findings

- There is no formal procedure for terminated employees and no repercussions for failing to change combinations and access codes, etc.
- There is no consistency across units with respect to requiring employees to sign their screening certificates.
- The record of screening levels is contained in a centralized PeopleSoft database. There is uncertainty as to the appropriateness of these levels.
- Computer authorizations are eventually removed when individuals leave, but there is uncertainty with respect to the efficiency of the process.
- The client can access the DPM Secur Security Clearance Processing System (SCPS) at the CFPM website.

Key Recommendations

- A standard termination checklist needs to be developed and applied uniformly across all units.
- A review and monitoring process should be implemented within the units to ensure screening certificates are signed, employees' screening levels are appropriate for their position, and employees have been properly terminated.

2.5 Security and Contingency Management



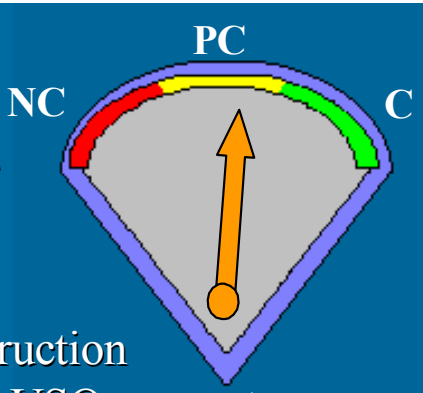
Key Findings

- Employees are unaware of their local emergency and contingency management plans.
- The majority of observed units have developed some sort of emergency plan. These do not, however, seem to be complete or tested on a regular basis.

Key Recommendations

- All unit personnel should be made aware of their resumption and emergency plans. If a local plan is not available, one should be provided (e.g. NDHQ plan).
- All plans should be regularly updated to reflect DND/CF's current environment and tested to ensure their successful operation.

2.6 Security and Contracting Management



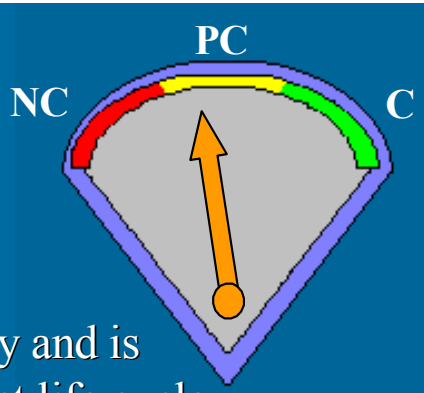
Key Findings

- Many units do not deal with contractors, as local construction engineering is responsible for contracting. As a result, USOs are not always aware of clearances for on-site contractors.
- Contract Security and Foreign Contracting is not fully covered in the NDSP, but will be expanded in the NDSI.

Key Recommendations

- Local units using contractors should take on the responsibility for ensuring that proper clearances are in place for all contractors.
- Contract security needs to be covered explicitly in the unit security procedures as it is a major issue.

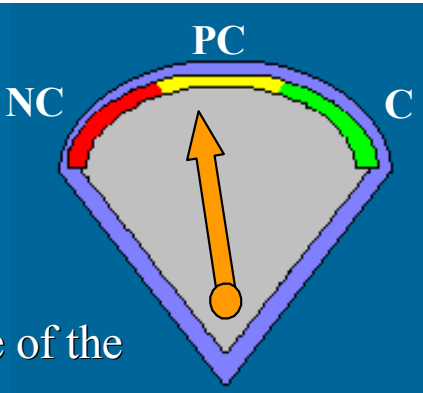
2.7 IT Security



Key Findings

- Security planning is not always perceived as a priority and is not always introduced in the early stages of the project life cycle.
- Monitoring and review is not consistent across units and tends to be reactionary in nature.
- Personnel and physical security is more or less compliant in all observed units, however, IT asset management could be improved.
- Many systems are operating without certification as the Certification and Accreditation (C&A) process is complicated and outdated.
- Software configuration practices are unstructured and inconsistently applied across units. The system security baseline is unknown.
- The security architecture is outdated.
- One unit visit revealed the processing of classified documents on a LAN printer, only approved for up to "PROTECTED."
- There is some concern over the insufficient monitoring of system administrator accounts.

2.7 IT Security (continued)

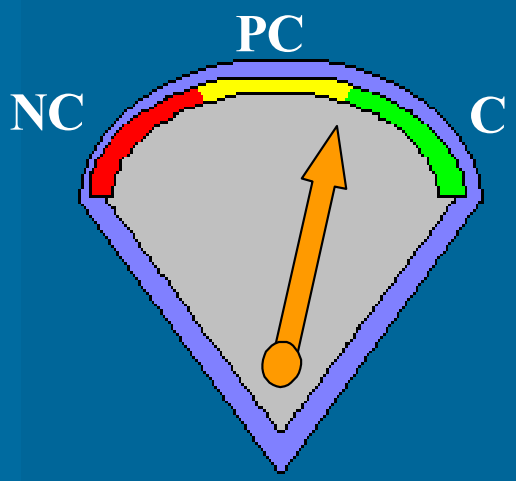


Key Recommendations

- Ensure IT Security is introduced at the planning stage of the project, with sufficient funding.
- The monitoring & review process should be standardized and proactive.
- Sensitive information should be encrypted on laptops, diskettes, etc. to minimize the risk of exposure in cases of loss.
- The C&A process should be updated to reflect DND/CF's current environment.
- Configuration management policies and practices should be developed and/or refined with department-wide guidance.
- The security architecture should be updated to reflect DND/CF's current environment and designed to minimize risk.
- Classified documents should be printed on stand-alone printers.
- All personnel with access to systems (e.g., systems administrators) should be appropriately monitored.

3.0 Conclusion

- Overall, DND/ CF was found to be compliant with the Government Security Policy (GSP).



- The GSP review identified several areas for improvement. The majority of these improvements were in the areas where partial compliance was determined. The recommendations put forward as part of the review will address these improvements.
- The main OPI in DND, CFPM/DPM Secur, has provided an acceptable management action plan that addresses review recommendations.

END OF KPMG SLIDE PACKAGE

MANAGEMENT ACTION PLAN

In response to this review, the main authority for this topic area, CFPM/DPM Secur, formed a team, which developed an action plan. The major aspects of this plan are presented below, grouped by the major categories of our review. Target dates and the OPIs within CFPM are specified where possible.

SECURITY MANAGEMENT

Reorganization (Central Focal Point) - Target date FY 2002/2003

A central focal point for guidance in security matters is already established. The central focal point is the office of the Departmental Security Officer (DSO)[6], and it is the primary function of that Officer to formulate and implement policy by addressing the needs of senior management for both the operational and business lines within the DND/CF.

This functional aspect has been lost through downsizing, re-structuring, and a general lack of awareness that the office exists and it's functionality. To address this issue, the ***DSO*** during FY 2001/2002 will:

- complete six staff visits to units wherein security deficiencies have been noted;
- schedule interviews with Level 1 managers to discuss and identify their security concerns and requirements;
- continue to identify both internal and external committees where the DSO and DPM Secur staff must have affiliation; and
- continue the implementation plan for the renewal of the Departmental Security Program.

Monitoring – Target Date July 2001

The essential framework required to achieve security reviews/inspections will be developed and identified within the Project Charter and the Implementation Plan for the Departmental Security Oversight Program. ***OPI - DPM Secur.***

Standardization – Target Date December 2001

The security policy revision of the current National Defence Security Policy (NDSP) will address the requirement for standardization of USO roles and responsibilities.
OPI - DPM Secur.

[6] The incumbent DSO is DPM Secur, reporting to CFPM as part of the VCDS organization.

Training – Target Date May 2001

Discussions will ensue with Canadian Forces Recruiting Education and Training System (CFRETS) regarding the qualification standards of the USO training course. ***OPI - DPM Secur***.

Awareness – Target Date April 2001

Discussions are to occur between DPM Secur and the newly appointed officer for the Resource Protection cell within CFPM, in order to promote security awareness issues. ***OPI - DPM Secur***.

SECURITY ADMINISTRATION

Policy and Guidelines – Target Date December 2002

A Classification Guide must be developed to assist the employees of the Department and the Canadian Forces in understanding the requirement for accurately identifying and classifying originated information/assets. This functionality has been inappropriately associated with the security field due to the association that the information/asset is assigned an identification marking known as a *"Security Marking"*. The DSO role is to identify within the policy the requirement for security marking and how to apply the *"injury test"* in order to determine if the information/assets requires marking due to being categorized as "within national interest" or "within interest other than that of national interest". It is incumbent upon Commanding Officers to have identified *"Subject Matter Experts (SME)"* within their organizations who are authorized to classify and release information/assets.

The overall purpose of a guide is that of a resource tool for originators to further assist in identifying subject matter areas/topics, which the Department has pre-determined a set sensitivity level necessary to safeguard said subject/topic. The development of such a guide will require the collaboration of various organizations and then an assigned manager to maintain the document. ***OPI - DPM Secur***.

Threat and Risk Assessment Policy – Target Date December 2001

Threat and Risk Assessment (TRA) policy will be amended to ensure that TRAs are being conducted regularly and reported to the proper authorities. The DSO is also exploring software packages which may provide a technical solution for both Security and Information Technology TRA requirements. ***OPI - DPM Secur.***

PHYSICAL SECURITY

Reporting

All USOs should receive security incident reports for their unit. Both the USO Role and Responsibilities and the Reporting of Security Incidents policies will address this issue in detail. It is also anticipated that this issue will be considered in conjunction with the development of the Results-based Management Accountability Framework (RMAF) for governance of the DND/CF Security Oversight Program.

Improved Reporting

Annual "State of Security" reviews and reporting by all units will be achieved in conjunction with the new National Defence Security Instructions (NDSIs), and the Departmental Security Oversight Program. The OPI and target dates will be set upon completion of the RMAF for the governance of this program.

Improved Control of Mobile Assets – Target Date December 2002

The requirement for sign-in/sign-out for mobile assets to make individuals responsible for the device and its content will be addressed as part of the new NDSI. ***OPI - DPM Secur.***

CONTINGENCIES AND CONTRACTING MANAGEMENT

A *"Security-in-Contracting Working Group (SICWG)"* has been formed by DPM Secur to address contractual security issues, and to enhance contractual procedure and awareness amongst departmental stakeholders in order to streamline and eliminate duplication. ***OPI - DPM Secur.***

INFORMATION TECHNOLOGY SECURITY[7]

Improved IT Security Planning – Target Date 31 December 2001

This issue will be addressed as part of the new NDSI and imposed by the GSP.
OPI - DPM Secur/CFIOG.

Improved Monitoring – Target Date 31 July 2001

The project implementation plan for the Departmental Security Oversight Program will address this issue. It is understood that CFIOG/IPC is also working towards the development of an oversight program for Information System Security (ISS). ***OPI - DPM Secur/CFIOG.***

[7] These actions relate to the compliance related issues raised in this report. Further action is anticipated in conjunction with the CRS review of DND/CF Information Security mentioned previously.

Safeguarding of Sensitive Information – Target Date 31 December 2001

The safeguarding of a valuable asset will be addressed within the applicable NDSI. This issue may also be resolved with the Public Key Infrastructure (PKI) framework yet to be fully developed by the Government of Canada and the Department. ***OPI - DPM Secur/CFIOG***.

Certification and Accreditation – Target Date October 2001

It is agreed that the Certification and Accreditation process within the Department is laborious and technically inclined. Therefore, there is a need for revision of the certification and accreditation process oriented towards concept and principles.

A working group shall be formulated to produce a new Certification and Accreditation Guide (CAG). ***OPI – DPM Secur/CFIOG.***